

LOAN DOCUMENT

PHOTOGRAPH THIS SHEET

①

LEVEL

INVENTORY

New World Vistas...
Information Applications Volume

DOCUMENT IDENTIFICATION

1995

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

DISTRIBUTION STATEMENT

H
A
N
D
L
E

W
I
T
H

C
A
R
E

NTIS		GRAM	<input type="checkbox"/>
DTIC		TRAC	<input type="checkbox"/>
UNANNOUNCED			<input type="checkbox"/>
JUSTIFICATION			
BY			
DISTRIBUTION/			
AVAILABILITY CODES			
DISTRIBUTION	AVAILABILITY AND/OR SPECIAL		
A-1			

DISTRIBUTION STAMP

DATE ACCESSIONED

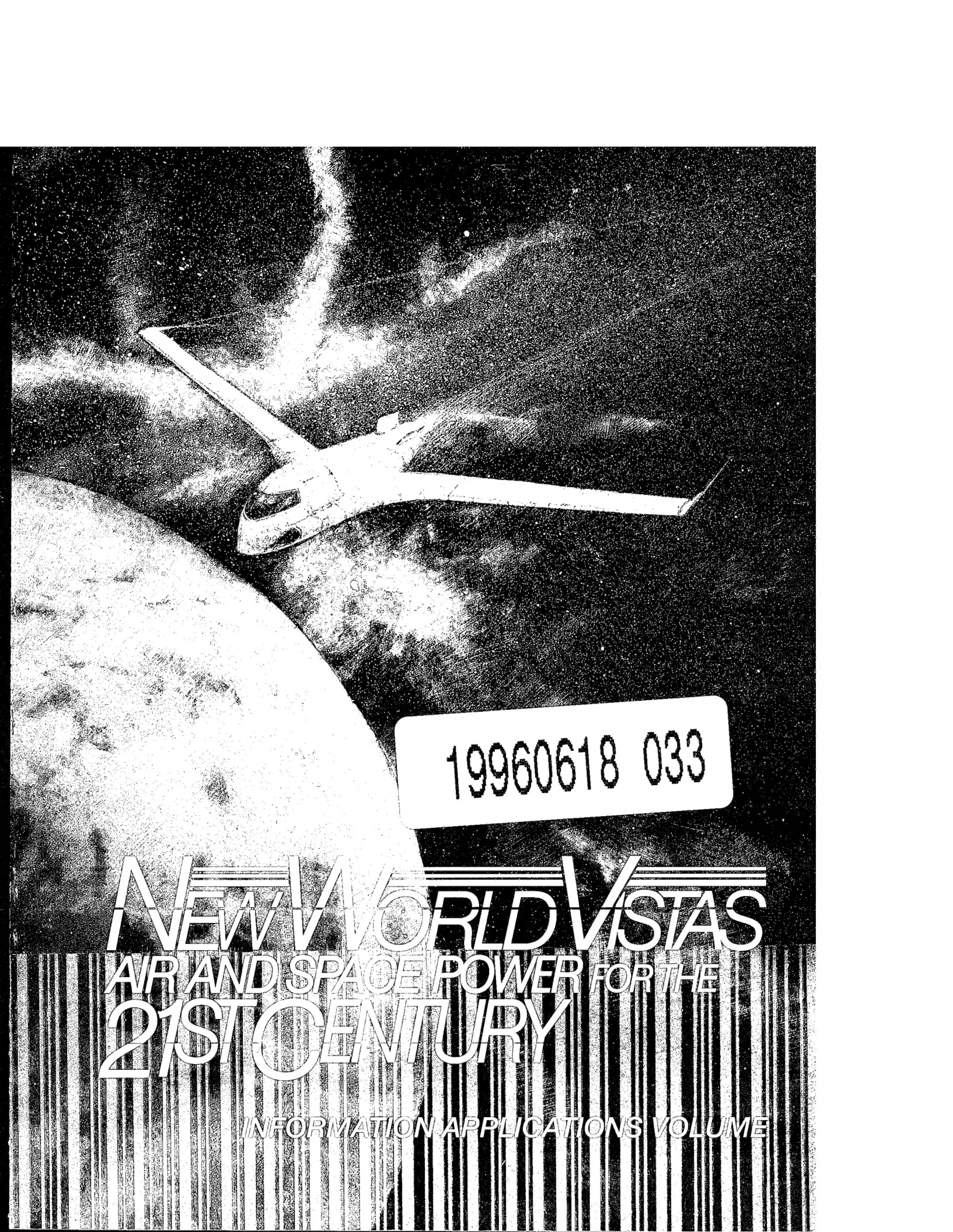
DATE RETURNED

19960618033

DATE RECEIVED IN DTIC

REGISTERED OR CERTIFIED NUMBER

PHOTOGRAPH THIS SHEET AND RETURN TO DTIC-FDAC



19960618 033

NEW WORLD VISTAS

AIR AND SPACE POWER FOR THE
21ST CENTURY

INFORMATION APPLICATIONS VOLUME

NEW WORLD VISTAS

AIR AND SPACE POWER FOR THE

21ST CENTURY

INFORMATION APPLICATIONS VOLUME

DTIC QUALITY INSPECTED 1

This report is a forecast of a potential future for the Air Force. This forecast does not necessarily imply future officially sanctioned programs, planning or policy.

Executive Summary

Air Force Information Applications in the 21st Century

Dr. Charles L. Morefield

Chairman, Information Applications Panel

USAF Scientific Advisory Board

New World Vistas Study

Victory in war goes to those forces with the most accurate *knowledge*, strongest *protection*, most robust *communication*, best *coordination*, *dominant* force structure, and most *dynamic* operations. In the thoughts that follow, we expand upon these facets of military power by describing information applications¹ that will be important to the Air Force in the years to come. This short summary introduces accompanying monographs written by individual members of the panel. Our monographs contain comments and recommendations that speak to each of the following goals for 21st century aerospace power:

- Get the right *knowledge*, to the right place, at the right time for all aerospace missions
- *Protect* all Air Force computers, software, and data, regardless of platform or location, particularly those involved in warfighting
- Achieve global *communication* between the air, ground, and space assets of the Air Force, as well as those with whom we operate
- Maximize the speed and quality of Air Force *coordination*, planning, and execution
- *Dominant* the information battlespace
- Develop doctrine needed for the use of information in *dynamic* command and control of joint forces

This introductory monograph also provides some comments on information science in the Air Force laboratory system.

Future War

The US Air Force, a young service, is about to experience its first paradigm shift. The arrival of the information age means that the Air Force has entered a period of great change, one that mirrors the social and economic ferment of the world around it. The causes of this change are rapidly expanding communications bandwidth and computational power, the foremost engines of economic and military competition in the decades to come. Airpower was the deciding factor in the shockingly one-sided United States victory in the Persian Gulf. However, the emerging information age requires new strategies, tasks, and technologies for exercising military power.

1. The reader is also referred to the work of the Information Technology Panel for a discussion of technical trends and research issues in the information sciences.

Beginning in 1940, and extending to the fall of the Berlin Wall, powerful currents of military competition drove the technologies most important for today's Air Force. At the edge of the millennium, the equally powerful engines of economic competition are hard at work. They carry us toward a future of ubiquitous computing embedded in a dense global communication grid, technology that will transform the Air Force (see Figure 1).

It appears now that nanofabrication technology will permit computer designers to maintain their hectic pace of greater capability, smaller size, and lower cost. Because of this, computers will disappear into the fabric of everyday life. We will wear computational devices like clothing, glasses and hearing aids. We will soon speak and gesture to them in natural ways, encouraging military reliance upon them to significantly increase. Huge commonsense databases linked to reasoning engines will provide ubiquitous intellectual assistance and entertainment in everyday life. Distributed knowledgebases linked to mobile reasoning engines will dramatically improve

the ability of the battlefield team to obtain information, collaborate, and act.

Fiber grids will soon connect all the world's cities, and orbiting cellular overlays may even sooner provide universal access. The information applications inhabiting these global nets will change the economic and social structure of the world. How the Air Force responds to this change will determine its future as a viable military service.

If the Air Force adopts a path that unites aerospace with the infosphere, it will provide the United States with immense new leverage in the world. These two domains share an important characteristic: presence and influence are focused very rapidly on a global scale. An information-based Air Force will retain for the United States its position as the premier global military power into the 21st century.

The Air Force will reengineer its sensors, platforms, weapons, and command centers around the use of new information technologies. Most businesses and elements of the defense establishment are moving in this direction, making it possible to share the development burden of the effort. By

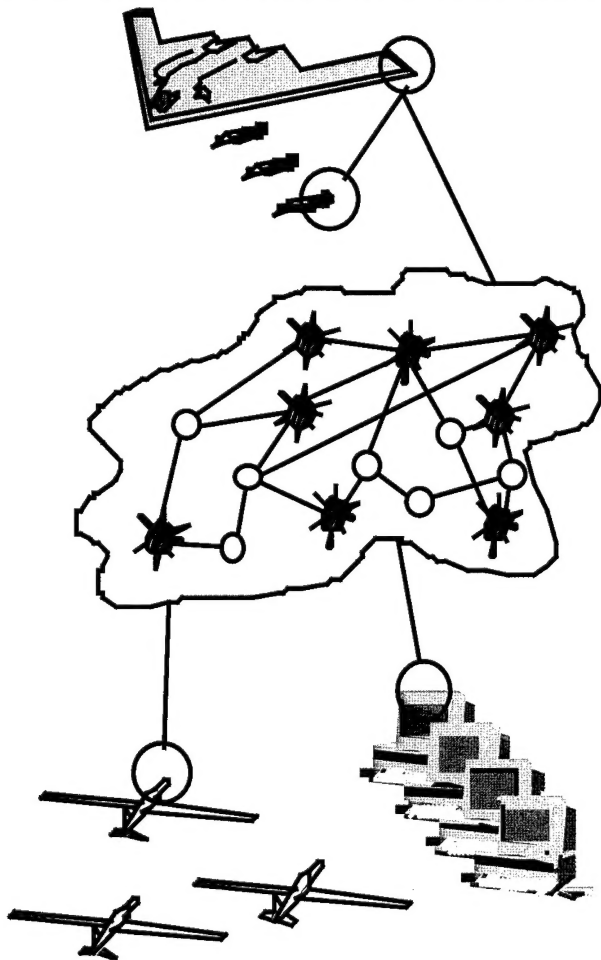


Figure 1. Telecommunications and computer technology will transform the Air Force

2025 (the notional end of this monograph), even the smallest artifacts of everyday life and cheapest weapons can have powerful embedded computers and sensors. The integration of such weapons, and the wide scale adoption of trusted automatic systems for information fusion and coordination, will change the face and pace of warfare.

Information Warfare²

Today's computer systems are a limited and sometimes frustrating portal into a patchwork of databases of varying integrity. In the 21st century, the infosphere will evolve into a much more powerful and useful information utility. As computers emerge that respond coherently to speech and gestures, the infosphere will become a pervasive tool of everyday life. It will become a meeting place for teleconferences, real time global situation assessment, automated decision support, and for management of the global battlespace. The infosphere will encourage new relationships:

- Pseudo-intelligent agents will interact in complex ways with human beings and with each other
- Manned aircraft will interact with smart weapons, smart sensors, smart spacecraft, and smart unmanned aircraft, as well as command and fusion centers
- Commercial knowledgebases for weather, intelligence, and surveillance information will become available within the infosphere
- Military users will come to rely ever more extensively on the global grid, commercial information providers, and commercial information technologies

For these reasons, *information warfare* will radically alter the tasks associated with putting energy on targets. Early in the next century, however, information warfare will also take place *within* the infosphere. Such warfare will extend beyond the military domain, and will couple to it in ways that we cannot now predict. Computer networks will tie the economies of the world together in critical ways. This will present attractive opportunities for competing global interests to develop automated information fusion and planning systems for both military and commercial purposes. The leading edge of this pattern is visible now as electronic trading of financial instruments, the commercial use of GPS, and automated transportation and tracking systems.

The degree to which the Air Force develops the professional expertise to engage in national policy debates, allocates research and development expenditures, and encourages a military doctrinal evolution will determine its future. Information objects contained solely within the infosphere will become as important as real objects in the 21st century. Digital cash, a powerful target recognition algorithm, a predicted drop in the S&P 500, or the current position of a military leader may only exist as objects in some computer's memory. However, they would be knowledge of great commercial and military importance.

2. We use the term *information warfare* in the following way: protecting and using to best advantage our own information operations, while attacking and exploiting opposing information systems. In this definition, information warfare includes command and control, surveillance, electronic warfare, protection, and other technical information operations. The term is also applicable to the protection of national and global infrastructure, including networks for electric power, telecommunication, finance, and transportation.

We require a clearer understanding of how software munitions will affect future wars. A rapidly increasing population of valuable information objects requires the United States to develop the tools to protect its commercial and military information systems. We should prepare ourselves for sophisticated software weapons operating solely within the infosphere, directed against our economic, social, and military institutions. The Air Force should prepare itself through its research programs for a key role in dealing with protection issues. Since it is first a military service, it must also have the means to respond to attack in a destructive way (or at least pose the threat of destruction).

Mutual assured disruption (MAD) within the infosphere will become a key point of policy debate. Because of the increased integration of the world economy, and the complexity of its information linkages, side effects of war within the information domain will be unpredictable. Even “restricted” attacks against one part of the infosphere may lead to unpredictable collateral disruption of money flows, transportation links, or other facets of 21st century life.

The doctrine of “mutual assured destruction” became a strategic cornerstone of the Cold War. Similarly, the fragility and importance of the world’s information infrastructure can lead to an equivalent doctrinal impasse. Such a policy event would not diminish the importance of information to other parts of warfare, nor would it relieve us from the need to protect our vital systems. Small interest groups (below the level of nation-states) may choose not to subscribe to MAD. Since information technology is universally available, such groups may use sophisticated software munitions as threats.

We must develop new defense policies that clarify our response to digital events. The dividing line between economic espionage and attacks against our homeland will begin to blur. Taking down a regional power grid by software attack, with its attendant loss of life, is clearly an act of war. Would it be an act of war to destroy the digital financial or technical records of critical semiconductor companies? How can we respond (particularly if we are unable to unambiguously determine the bad actors)?

The Revolution in Military Aerospace

Dealing with information warfare in a fundamental way will cause a profound cultural shift in the Air Force. This shift will begin in earnest over the next decade, and may be wrenching for those imbued with the cultural heritage of manned aircraft. It will come at a time of increasing use of unmanned aerospace vehicles, widespread interest in information warfare issues, and changing roles and missions among the services and agencies of the United States defense establishment. We must integrate aerospace military strategy with the information rich techniques that will dominate future battlefields. We should extend our functional capabilities in situation assessment, battle management and simulation to encompass objects within the information battlespace.

To respond to these changes, the Air Force must expand its traditional role as the leading proponent of airpower to include the infosphere. To the extent the Air Force can effectively unite aerospace power with information based power (networking, sensors, fusion, coordination, protection and other capabilities), it will remain a dominant factor in the defense of our nation. We should establish carefully thought out goals, goals responsive to the evolution of technology

and other commercial and government institutions. We must carry out difficult comparisons among the competing requirements for manned aircraft, space, and the informational components of force structure.

Issues Affecting Air Force Battlefield Information Applications

Military designers increasingly focus on *minimizing* the detection of friendly platforms, while *maximizing* the detection of enemy targets. Ever increasing volumes of multi-source global surveillance data from unmanned aircraft, ground and sea sensors, national, and open commercial sources are available to support the detection function. Since human processing of this magnitude is not possible, the Air Force will need to replace manual information processing with intelligent automation. As a corollary, the high processing load will require the Air Force to use network-based, scaleable computing resources to accomplish fusion.

Among larger nations, aerospace warfare will eventually be dominated by forces possessing the best:

- Stealthy air, ground, and space delivery systems able to prosecute maneuvering and non-maneuvering targets
- Ability to detect and suppress air defense systems, cruise missiles, ballistic missiles, satellite attack, and digital attack
- Ability to attack important ground facilities mixed in with civilian populations, and obscured by camouflage and movement
- Ability to fuse a diverse mix of sensors
- Ability to rapidly coordinate complex missions involving precision attack
- Ability to protect its information assets, while attacking those of its opponents

In a short time every nation (and small interest group) will have access to:

- Orbiting wireless communication switches integrated with the global fiber grid
- Commercial satellite surveillance and navigation
- Public networks of increasingly powerful computers and sophisticated software
- Commercial multimedia knowledgebases

Both micro wars and major regional contingencies have become information intensive conflicts. As a corollary, warfare will emerge *within* the information domain driven by the proliferation of computer technology, low cost of entry, and large numbers of attractive military and civilian targets. Even small interest groups can develop the systems integration skills required to build niche military capabilities. Feasible specialties include information systems, wide area weapons, ground-to-air missile systems, cruise missiles, and unmanned aircraft. They will become adept users of the global telecommunications grid, commercial navigation and surveillance satellites, open source knowledgebases, computers and software, commercially available surveillance components, and exported weapons.

Low cost of entry will encourage the emergence of one or more small nations focused on information warfare. They will carefully shape their legal systems to support this activity. Even small interest groups will find this attractive, given the available cheap infrastructure (for example, satellite data services, global fiber grid, cheap computers, ready availability of highly trained computer scientists). Because of this, others will replicate key parts of the US military advantage.

Within our own military and economic spheres, other changes are taking place. These include integration of our national/airborne/commercial surveillance resources, the emergence of a civilian space surveillance industry, and the increasing reliance of the US military on internationally produced electronics components.

Current Air Force Communications

The Air Force currently organizes its airborne data links around three paradigms:

- Tactical links: local area multiple user networks, and modems attached to low bandwidth point-to-point voice channels
- Dissemination links: low bandwidth wide area data broadcasts
- Collection links: higher bandwidth point-to-point linkages

Current airborne data links have thin, inflexible airborne service layers³ focused on encrypted and anti-jam connections. This puts the responsibility on users to provide custom solutions for their needs, and does not provide scaleable bandwidth, user driven network management, or other services. Wide band fiber and satellite links provide near-term ground connections to bitways.

Service layers for ground nodes (and some wide-body aircraft) are beginning to mirror commercial standards. Important strides are being made in adapting commercial open standards to workstation-based applications. New airborne systems represent our first opportunities for airborne open software standards in embedded systems.

Air Force airborne tactical data links have historically been constrained by cost and lack of clear doctrinal necessity. The near future is being largely determined by:

- An Air Force decision to equip many fighters with voice radio modems
- The Air Force experience at Mountain Home Air Force Base, Idaho (and DoD mandates) supporting a standard local area data network for aircraft and other mobile platforms
- Emergence of air warfare doctrine supporting real time information flows into the cockpit, supported by experimental trials of onboard information systems
- DoD interest in wide area data broadcast systems

The bitways connecting ground based systems derive in part from Cold War legacy systems, but are rapidly being supplanted by the commercial global grid and the evolution of government furnished infrastructure. The service layers for ground based systems are a mix of new commercial

3. *Service layers* consist of software that provides a standardized means of managing the raw bandwidth provided by a data link.

and custom legacy systems. There is rapid movement toward commercial open system standards, and toward use of commercial network services within a military context.

Current Information Applications

Current military information applications are custom designed for each platform and mission. Legacy hardware substrates are increasingly replaced by workstations or powerful embedded commercial microprocessors. There is little direct coordination of information applications among participating computers and functions. However, merger of information applications across individual programs and missions is beginning to rationalize the overlap among legacy applications (for example, mission support systems for pilots). Fusion systems are hand-tooled and have low levels of automation. Coordination systems are large and unnecessarily complex.

Substantial research has been focused on automated fusion and planning systems, but successful fielded applications are still largely manual. Current automated systems (e.g., for model-based target recognition and multitarget tracking) are fragile devices that will require substantial research investments before trusted implementations become available.

Current and near future Air Force and DoD ground-based information applications are evolving through the merger of numerous legacy command, control and intelligence systems. This will leave in place large, complex analyst-intensive approaches to both fusion and coordination. It will also let stand a confused information architecture.

Lacking integrated bitways, service layers, or integrated applications architectures, today's information applications are isolated, platform centered designs. Even the newest Air Force platforms accept this approach.

A Long Term Vision for Air Force Information Applications

Given this background, what is the appropriate direction for aerospace information applications? The issues split into several parts:

- What are the doctrinal imperatives the applications should serve?
- What communication designs are affordable?
- What protective services are feasible?
- What information applications should operate across the system?

The Air Force has yet to accomplish a careful long term look at the impact that extensive reengineering of its information systems will have on air warfare doctrine. The primary areas now discussed are wide area broadcast and air campaign management. The issues go deeper. For example, will the Air Force need planning and battle management assets in the theater of operations? (Data links could substitute for on-site presence.) How are all assets (aircraft, spacecraft, sensors, communication links, joint and allied resources) managed? (Integrated and joint warfare imply some loss of autonomy.) How quickly can the Air Force employ its tactical air power? Should command and control follow a horizontal model? (It could, when global nets become available.)

The communication pathways of the future Air Force should include a netted airborne information system that supports a wide range of military tasks, available on a global basis for any task or mission. Figure 2 illustrates some of the physical bitways of such systems. Numerous data channels could be available in this network, including:

- Globally available broadcast channels (a wideband satellite downlink with many available channels)
- Globally available two-way data channels (multiple access wireless connections to a worldwide digital network)

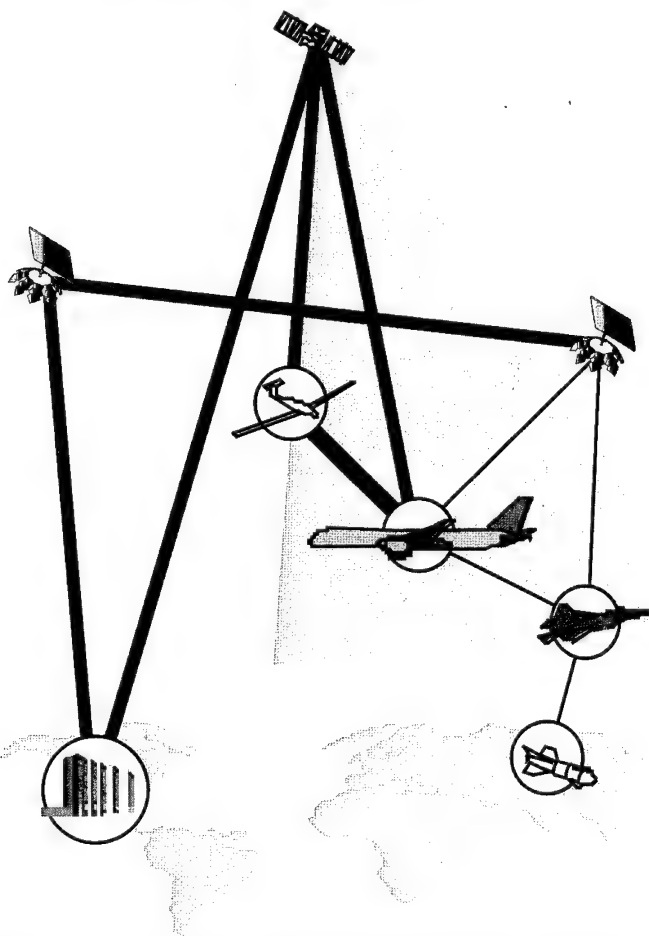


Figure 2. Future data links between aerospace platforms

Two-way data links to aircraft in flight are harder to develop than the broadcast link discussed above. A flexible, globally available multiple access two-way data channel should be able to do many things. For example, a weapons controller at Langley Air Force Base could open a data link to an aircraft in flight anywhere in the world. The controller could (for example) see a replication of the cockpit instruments, stores, and the onboard situation displays. The

Wideband broadcast links are under consideration in a number of government activities, and used daily in commercial digital television broadcasts. This type of channel could provide a "push" or "knowledge by design" or "immediate warning and control" type of link. Replaying constantly the current situation updates, it would provide the ability for a weapons controller to immediately reach an aircraft that is controlling emissions. (In many cases, military aircraft may not want to transmit, yet still receive some type of knowledge flow into the cockpit.) It would, for example, give a controller or other source of critical information the ability to warn a pilot of an impending surface-to-air missile attack. Pilots would adjust their pre-flight filters with access keys to select channels corresponding to their needs.

channel would provide a digital connection to any aerospace platform (satellite, aircraft, ground center) maintained in real time between two or more points around the globe. This would provide a “pull” or “collaborative” or “knowledge on demand” type of link. Links of this type, if global, would require some combination of satellite and unmanned air vehicle transponders. An unprotected commercial version of this system will be available for Air Force use if currently proposed satellite systems are built.

The communication pathways will have a layer that includes protection and other services. The communication links will be wrapped in protective walls of software and monitored by software warriors that police the fabric of the net. As part of the service layer, software agents⁴ could talk to one another in a coordinated fashion. Software facilitators between the pilot and information agents will manage the flow of knowledge to cockpit displays, thereby avoiding information overload.

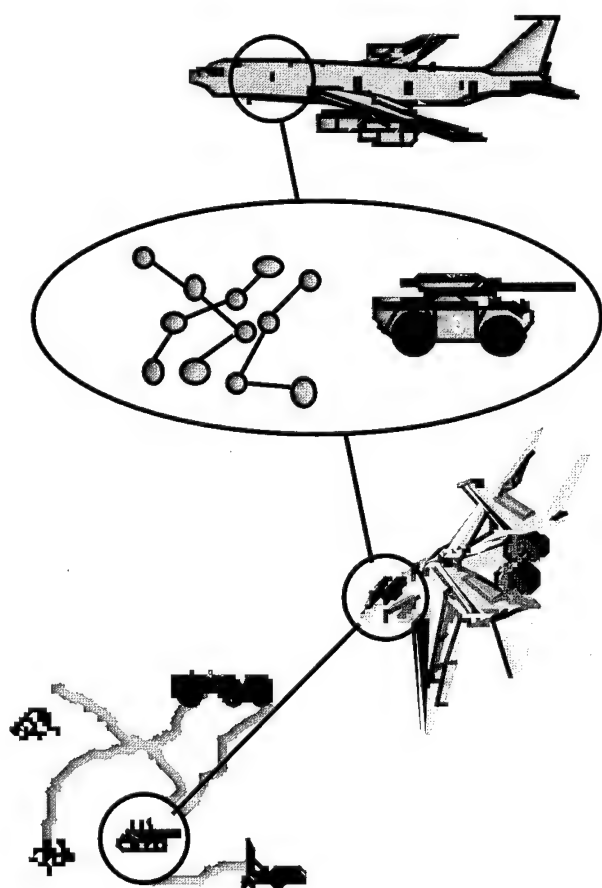


Figure 3. Distributed data fusion

Embedded within the net will be facilities that present a rich and accurate picture of the world. These will be drawn from a global array of sensors, many carried on aerospace platforms. Automated fusion will distill this overwhelming flow of data into a meaningful collection of information. The system will include many automatic fusion engines, distributed to many locations across the net (see Figure 3).

Since speed will be of the essence in future wars, automated coordination assistance will be required. The goal should be an information driven Air Force that relies upon global situation awareness to plan and execute complex missions quickly and accurately, with minimum danger to its personnel.

The Air Force Research Laboratories

Parts of the research and development goals listed above are already being pursued within numerous research groups, including the laboratories of the US Air Force. How well equipped are these USAF research groups to achieve our suggested long term goals?

4. See the Information Technology Panel's monograph for a discussion of software agents.

The last few years have seen the fracturing, consolidation, and down-sizing of some of the key research institutions supporting the US military. The Air Force laboratory system has not been exempt from this. Continued down-sizing is inevitable. It is mirrored by a similar trend in allied private research institutions, as their historic business models are called into question by their sponsors. In addition, the major universities that have provided long term ideas in information sciences are being drawn to a shorter term focus through fiscal pressures. This trend will continue for some time, and will shrink significantly the research base under the direct influence of the Air Force.

The Air Force must respond to this with a long term technology strategy for those areas that it will continue to directly support. Not all of these will represent areas of current strength, since the relative importance of individual technologies changes over time. Thus, the Air Force may sometimes face the unenviable task of down-sizing a strong technical group that has become less relevant, to make way for a different research focus.

Regardless of physical location or management format, the Air Force must retain an ability to fund and manage research in the information field. The implication of ubiquitous computing is that information systems will be part of every Air Force research and product development group. It is likely that this distributed approach to the information domain will be continued. This may cause a reallocation of funding among research groups at different locations, depending upon the requirements and decisions of Air Force leadership.

Coordination Among Laboratories in Key Research Areas

It is also important that the research be *coordinated* in key focus areas, such as in the research threads for information fusion discussed in the paragraphs above. Several of these can and should be carried out in coordination with a mix of government, university, and industrial fusion research groups. For example, the fusion systems supporting situation awareness have many common characteristics, whether carried on a ship, helicopter, satellite, fighter, or surveillance aircraft. Common research goals should be established in this area across the numerous groups with a present requirement or capability in fusion. Common goals will draw the government, university, and industrial research base into a more stable long term configuration. Focus groups can be established to support airborne avionics, satellites, weapons, and command and control activities. In fusion research as in aerospace missions, coordinated planning with decentralized execution will prove key to the attainment of difficult goals.

The Air Force needs particular assistance in the development of cheap global mobile communications suitable for use on military aircraft. Government programs, such as those in progress at the Advanced Research Projects Agency, should be pursued aggressively. They provide a unique window for the Air Force into cheaper mobile communication technology (indeed, into many of the key research goals listed above). Much greater use should be made of communications research in institutions aligned closely with the commercial world.

Coordination Between Air Force Leaders and the Laboratories

Research at Air Force labs has not always flourished under Congressional scrutiny in recent years. Part of the reason for this is the natural ebb and flow of opinions of our nation's leaders, and the economic situation in which our nation finds itself. However, the time is ripe

for a careful rethinking of laboratory emphasis. In the information domain, three things would be helpful:

- A more complete strategy for extensive use of commercial information systems technology
- A much longer term viewpoint for the Air Force's internal plans for specific mission areas
- The adoption of a research strategy that matches the long term commitment of Air Force leadership to field particular types of capabilities (see Table 1)

Commercial needs will dominate the evolution of many technologies important to the Air Force. For example, commercial mobile bandwidth is becoming ever cheaper for business users, but remains expensive when bought as military airborne systems. An adoption path for use of emerging commercial technologies on military aircraft could be built around programs underway both inside and outside the military laboratory system. Phased array antennas, software radios, and satellite broadcast television are examples of such technologies.

The Air Force should make a strong effort to match research programs to the serious long term intent of Air Force leaders. Extending the period covered by mission area plans would permit research goals to be meaningfully related to the needs of the Air Force. We have offered several long term research goals above. Funding limitations imply that laying a stronger emphasis on the items listed above will lead to program reductions in other areas. The Air Force should give much thought to its long term objectives, however they may be selected, and focus its research groups on these key goals in a very clear way.

Can Radical Changes Help in the Information Sciences?

Most of the research goals listed above will take years to achieve. Patient, stable research programs matched to clearly enunciated long term goals will allow the Air Force to dominate the information sphere throughout the 21st century.

With a long term view in mind, how can the Air Force attract high quality officers and civilians with an information sciences background? If information is the key to the future, qualified professionals will be required. Thought should be given to attracting graduates of major universities with strong information science programs. This could be done through an Air Force ROTC program established at a university recognized for its leadership in information sciences. In return for service in the Air Force, undergraduate scholarships could be granted. In this manner, it would be possible to attract young motivated individuals into service. These individuals would not be oriented toward flying airplanes, but would be slotted from the start for active leadership roles in key laboratories and command and control facilities.

Would it be appropriate to consider alternative business models for a portion of the Air Force laboratory work in information science? One model for doing so is the Advanced Research Projects Agency, which operates in part with a management that is drawn for a limited period from industry and the universities. Focused on vanguard technologies, such a program management staff could initiate and maintain a momentum for the Air Force in these areas. The Air Force might locate such a program management staff near a major university strong in

information science, with a view toward pursuing focused programs of long term interest to the Air Force.

Key Recommendations of the Information Applications Panel

Our primary recommendation is the following:

It should be the goal of the Air Force to achieve information dominance to enable the execution of its missions through the unconstrained but protected use of the infosphere, including segments that the Air Force does not control.

This goal has several elements, outlined in Table 1. Each entry of Table 1 corresponds to monographs written by panel members.

Table 1. Recommendations of the Information Applications Panel.

- **Get the right knowledge, to the right place, at the right time for all aerospace missions--** "Situation Awareness in the 21st century" (research directed toward automating the tasks of data fusion)
- **Protect all Air Force computers, software, and data regardless of platform or location, particularly those involved in warfighting--** "Defensive Information Warfare in the 21st century" (research into the issues of computer security)
- **Achieve global communication between the air, ground, and space assets of the Air Force, as well as those with whom we operate--** "Communications and Networking" (research associated with the evolution of the Air Force toward a densely internetted environment)
- **Maximize the speed and quality of Air Force coordination, planning, and execution--** "Coordination, Planning, and Execution in an Information Rich World" (research supporting new capabilities for command and control)
- **Dominate the information battlespace--** "Information Warfare in the 21st century" (steps toward an Air Force view of information warfare)
- **Develop doctrine needed for the use of information in dynamic command and control of joint forces--** "Information in Warfare: Toward Dynamic Command and Control" (thoughts on the participation of the Air Force in future Joint operations)

What should be done in the near term? What are the longer term research goals? The individual monographs record our detailed ideas. Some critical extracts are listed below:

- Fusion short term: increased speed in key fusion applications through operator cueing
- Fusion research goals: automated fusion
- Protection short term: protect all Air Force computers, software, and data following best commercial practice and military security policy
- Protection research goals: strong security for netted computer systems
- Communication short term: increased number of airborne platforms with data communication links, better interoperability, global dissemination broadcasts
- Communication research goals: cheap two-way global communication between all Air Force platforms

-
- Coordination short term: construct a system prototype that includes automated planning and scheduling tools, and hierarchical modeling and simulation
 - Coordination research goals: a distributed collaboration system that marries real-time automated planning with globally connected human interfaces
 - Information Warfare short term: develop an Air Force view of information warfare, and develop the software tools needed to monitor military infosphere
 - Information Warfare research goal: a rigorous fundamental understanding of the possible futures for software munitions
 - Dynamic command and control: near-term investments are needed to integrate doctrine with technology for joint warfighting

Speculating About the Future

This summary introduces the Information Applications Panel's monographs. Our emphasis throughout is on the long view. Our ideas and system concepts, if adopted by the Air Force, will require years to accomplish. To Air Force leaders who may look through these monographs: before you read our thoughts, read a good science fiction novel (Neal Stephenson, Bruce Stirling, or William Gibson come to mind). In doing so, you will see how very conservative our thoughts about the future have been.

Throughout the history of the Air Force, the discipline of physics has greatly influenced the thinking of its leaders. Today, many of us accept the idea that we live in the age of information. We have built the thoughts of our panel around this idea, as have other panels in the New World Vistas effort. However, think about this: most of the papers in the periodicals *Science* and *Nature* are not devoted to information science. They are devoted to biology.⁵ The intersections of these three worlds (physics, information, and biology) are many. For example, we see a potentially important thread in Len Adleman's recent use of deoxyribonucleic acid (DNA) to carry out computations analogous to those needed for automatic information fusion and planning.⁶

We are passing from a world dominated by physics, through one dominated by information, toward one dominated by biology. Biology will likely change our future more profoundly than physics or information science. The paradigms that inform our thoughts on military matters will shift, and (perhaps) shift again over the professional lifetimes of those entering the service today. The Air Force is a young military service, and information science is only the first of the paradigm shifts that it will experience in the 21st century.

Many thanks to the Information Applications Panel membership for their hard work and dedication to our joint task. The leading edge of the millennium is a great time to be thinking about the future. We have all tried to write documents that reflect our honest assessment of the future.

Chuck Morefield, Beckman Center, 1995

5. See the monographs by the Human Systems/Biotechnology Panel.

6. See the accompanying monograph "Situation Awareness in the 21st Century" for a discussion of DNA-based computation.

Contents

Executive Summary Air Force Information Applications in the 21st Century	iii
1.0 Situation Awareness in the 21st Century	1
2.0 Defensive Information Warfare in the 21st Century	17
3.0 Communications and Networking	32
4.0 Coordination, Planning, and Execution in an Information-Rich World	47
5.0 Offensive Information Warfare in the 21st Century	66
6.0 Information in Warfare: Toward Dynamic Command and Control	72
Appendix A Panel Charter	A -1
Appendix B Panel Members and Affiliations	B -1
Appendix C Panel Meeting Locations and Topics	C -1
Appendix D List of Acronyms	D -1

Illustrations

Figure 1 Telecommunications and computer technology will transform the Air Force	iv
Figure 2 Future data links between aerospace platforms.	x
Figure 3 Distributed data fusion.	xi
Figure 4 Current fusion architecture	3
Figure 5 An example of a coherent future architecture	3
Figure 6 Fusion and sensor systems will monitor the military infosphere	4
Figure 7 Multisensor fusion	7
Figure 8 Core technologies for the fusion (more important denoted in bold)	8
Figure 9 Fusion systems constructed to a common reference model, operating in concert across a computer communications network.	11
Figure 10 An unbounded domain viewed as a collection of bounded systems	21
Figure 11 Relationships among threats.	28
Figure 12	33
Figure 13 Global Networks for Tactical Theater Operations	33
Figure 14 Connectivity Requirements for Future Air Force Communications Network.....	35
Figure 15 SATCOM Systems.....	38
Figure 16 The C ⁴ I System of the Future	48
Figure 17 C ⁴ I Security Is Critical to Operations	50
Figure 18 The Many Faces of Architectures	55
Figure 19 The Geospatial Reference Grid	57
Figure 20 Intelligent, Distributed, Collaborative Planning	58
Figure 21 Intelligence flow	76
Figure 22 Requirements and response flows	77

Tables

Table 1 Recommendations of the Information Applications Panel xiv

Table 2 Threats and Countermeasures22

1.0 Situation Awareness in the 21st Century

Dr. Charles L. Morefield

Situation awareness depends upon trusted fusion⁷ software, good sensors, adequate communication links, and an effective display capability. Early in the 21st century, the Air Force will be capable of developing *automated* fusion technology for its command and control centers, aircraft, and satellites. Automated fusion technology will also be directed at the military infosphere itself.

In the view of some, appending the word “automated” to the word “fusion” constructs an oxymoron. This is largely due to the long history of failure associated with such systems in 20th century military applications. Indeed, success in this area will be difficult, and will require coordinated research programs that span several engineering and scientific disciplines. The focus of this monograph is on fusion algorithms and their associated software. However, the future success of automated fusion systems depends in fundamental ways on improvements in communications (data links and compression), computer protection, and sensors.

Fusion technology has not yet addressed the issues of situation awareness within the infosphere: how can we both monitor the information flow of our military infosphere, and automatically determine its evolving configuration? The technical challenges are complex due to our need to monitor the military infosphere without crossing the privacy boundaries our nation guarantees its citizens. Many top level tools of fusion are applicable to the infosphere since they derive from general principles of information interpretation. However, most of the lower level tools and sensors still await development. It will be particularly important to develop adequate human computer interfaces and simulation tools. They will be critical in actual operations and training, as well as the research process.

This monograph describes several aspects of the data fusion problem, and suggests useful research threads for the Air Force. It provides a short survey of a broad topic, and leaves out many issues that a longer paper would address. However, this paper does address certain issues of particular importance to the Air Force:

- Sensor volumes have already reached the point where automation is needed, since human operators alone are not capable of evaluating all information available on the battlefield
- The increasing pace of modern warfare requires more automation
- Research should be focused on the task of monitoring our own military infosphere in order to protect it against both peacetime and wartime threats
- Slow but steady progress is being made in important areas, but research must be consistently funded over a very long period to reach the goal of automated fusion

7. We use the term *fusion* in a very general sense: the evaluation of data from one or more sources to extract knowledge about events or objects of interest. We will use the term *fusion* when even a single sensor is involved.

The Broad Themes of Fusion Technology

Fusion research has a long history: several decades as a well-defined technical specialty. It began as a set of mathematical techniques applied to aircraft and missile tracking. Its techniques are rooted in probability theory and optimization. Over the years, many of its technical problems have attracted the interest of workers in the field of artificial intelligence.

It is important for the Air Force to provide new capabilities for data fusion. Research can leverage commercial technology, capturing the momentum of computer power and bandwidth, as well as the continuing evolution of commercial tools and standards for software design. In addition, the fusion community's large body of existing theoretical work provides a reasonable starting point for future work.

Data fusion involves several key tasks:

- Identify on a non-cooperative basis sufficient militarily significant targets and threats to establish an accurate real-time picture of the battlespace
- Locate targets, threats, and friendly forces with sufficient precision to support attack with available weapon systems
- Obtain sufficient situation awareness to support attack vs. threat avoidance decisions
- If attacked, understand in time to respond
- Do all the above within the threats' decision loop.

This monograph addresses the development of tools to carry out these important military tasks. There are several general observations that can be made about fusion and its relationship to Air Force operations.

Observation 1: Current information architectures supporting battlefield situation awareness are confusing. On occasion, late or incorrect information is presented to operational users. Architecture is dictated by the preference of both the operator and producer communities for autonomous execution of their roles and missions.

Workstations supporting manual fusion represent the dominant thread of fusion research. Factors that have influenced current designs include:

- Absence of an integrated battlefield information architecture
- Conflicting goals among producer and user communities
- Lack of interoperable data links
- Delays associated with manual fusion
- Security policies

Current *architectures* involve the interactions of multiple, often overlapping fusion products (see Figure 4). Products propagate through the reporting systems with different speeds, leaving conflicting viewpoints in the minds of key participants involved in battle management and execution. Biased fusion products may result from the duplicative use of underpinning sensor data. Such architectural confusion may place too much emphasis on certain objects

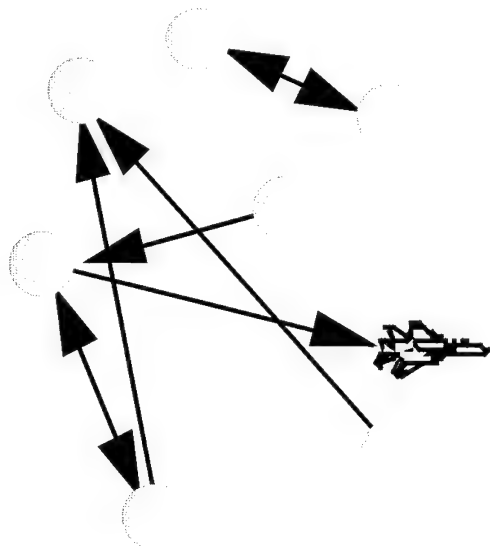


Figure 4. Current fusion architecture

high confidence broader views. The producer community has (for good reasons) traditionally resisted the dissemination of information without very careful evaluation of its accuracy. Such considerations take time, frustrating end users in the heat of battle. The user and producer communities are currently discussing how to bridge these conflicting needs. They will enjoy greater success if both sides permit software mediation of the fusion process.

causing duplicative reporting, or may lead to conflicting evaluations of the same object. Anecdotal stories abound, such as duplicative reports of missile launches. Future architectures need to be more coherently designed. In Figure 5, for example, each platform contains fusion software, and there are clear interactions among the fusion systems. The long term view shown is only one of many feasible coherent designs. The architectural paradigm shown (tree-like pathways to integrated fusion products) would work well in a very automated environment. Other sensible distributed fusion architectures are possible.

Conflicting goals have driven the evolution of battlefield information systems. Producers want wide consensus and integration before releasing information. Some users need a single vital datum immediately, while others need

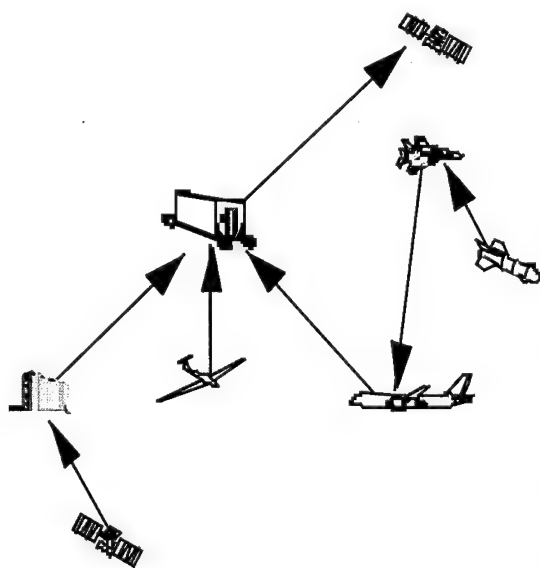


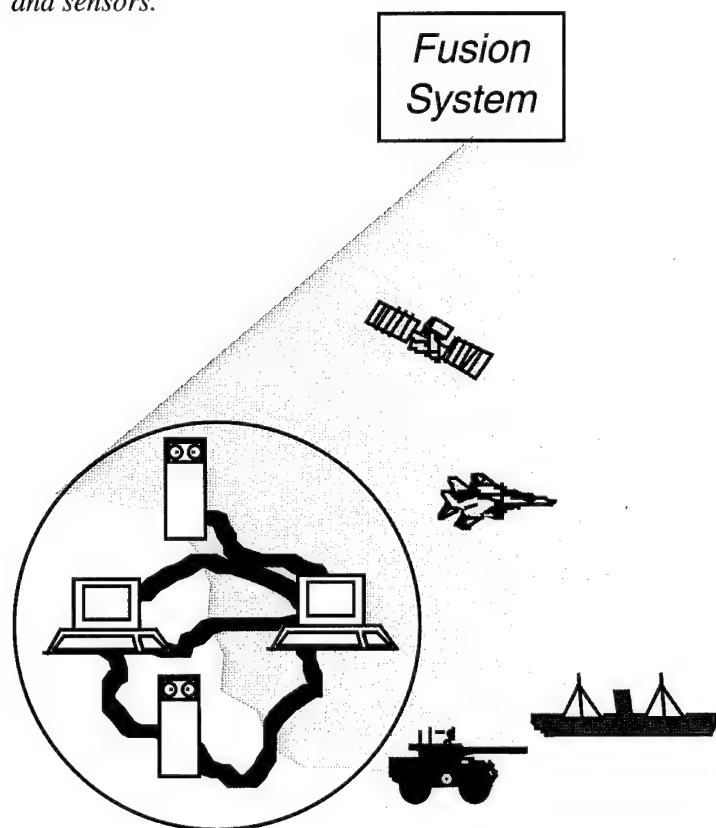
Figure 5. An example of a coherent future architecture

Data links continue to be a critical missing piece of the puzzle. We describe in other monographs a long term vision for Air Force data links. In the short and intermediate term, the Air Force already has plans to improve its connectivity. Adoption of community standard broadcast, tactical, and collection links is useful, although present versions of these links are expensive and less flexible than desirable. However, without thoughtful near term and intermediate term link planning, it will not be possible to improve situation awareness to the Air Force's satisfaction.

Queuing delays will continue as an issue in even well connected systems. The main thrust of the technology described in this monograph is automation of the fusion process, since this is the key technology for speeding up the dissemination of situation awareness information.

Security models will continue to place limits on the speed, accuracy, and wide dispersion of knowledge on the battlefield. Lacking key information, even the best analyst or fusion device reaches poor conclusions. Security (or lack thereof) has played an important role in 20th century wars, and will continue to do so in future wars. However, it is important to understand that the technical translation of security into software for situation awareness can drive architectures away from their optimal configuration by introducing quirky technical artifacts.⁸ The easiest way to dispense with such issues is to give every reported fact the same security label (as is sometimes done in wartime). Absent such a possibility, we must deal with security so that that information products are not factually misleading to the end user. This will remain true even when multilevel secure systems are available.

Observation 2: Automatic fusion systems are needed to monitor the military infosphere. The advent of software munitions will require the development of new data fusion methodologies and sensors.



Wide area computer networks have already become important for military purposes. As the military infosphere continues to evolve, a pressing need has emerged to see and understand software events as they unfold (Figure 6). Monitoring for context and intent is important for both peacetime and wartime use of the military infosphere. Current tools supporting fusion in the infosphere are very elementary. Many current tools require manual intervention and interpretation. Long term research will be required to develop automated means of advanced warning and attack assessment. As in classical applications of fusion, multiple software sensors will be required to track moving objects through networks, and to identify individual objects from their observed characteristics.

Figure 6. Fusion and sensor systems will monitor the military infosphere

8. Technical designs that mimic (in software) the historical US security approach include the Bell-LaPadula model. This well known model (whose adequacy is still debated within the software community) reaches an occasional impasse that impacts the fusion process. For example, it requires blind writing to databases when moving from a lower to a higher level of security.

Observation 3: Attempts to automate fusion for aircraft avionics and other difficult applications have not been widely successful, leading to great skepticism about its use on the battlefield.

Dependable knowledge of the battlefield comes from the fusion of disparate information carried by communication systems of varying capabilities. Limitations in the quality and flow rate of incoming data, as well as limitations imposed by computer power and security, make *automatic* fusion very difficult. However, we are approaching an era when development of automated fusion systems will be enabled by the evolution of computers, improved sensors, and more robust communication systems. It is not yet clear that the security models adopted for these systems will evolve sufficiently to support automated fusion.

Rigorous technical approaches to automated fusion are often couched in heavily mathematical terms. They use evaluation metrics, drawn mainly from probability theory, to guide the search for an accurate fusion product. These metrics are based in turn on detailed physical considerations (for example, radar reflectivity or Kalman filter motion models).

Complete automation of this process has failed so far because of its immense computational requirements, and because robust interpretations of sensor data are hard to develop from mathematical considerations alone. (These comments apply equally to one-, two-, and n-dimensional sensor data.)

To arrive at accurate fusion products, analysts involved in manual fusion intuitively select certain mental models and tools based on their evolving situation viewpoint. As time goes on, this activity (commonsense reasoning about the *process* of fusion) can be automated. Commonsense reasoning systems to manage fusion tools are an important goal for fusion research to seek. If feasible, they will provide an important improvement in the speed and volume of fusion processing.

Data fusion technology will become particularly important to the Air Force as new 21st century threats emerge. The set piece strategic warfare of the Cold War is giving way to a patchwork of many different threats and levels of engagement. The task of adjusting the parameters of our information systems to match enemy targets will be more difficult as the stable military equipment configurations of prior years give way to greater diversity.

Robustness (with respect to changes in target parameters) is key to effective military use of these powerful technologies. Therefore, variations in military equipment will be among the critical factors in evaluating the utility of new model-based fusion systems for signals and images. Current fusion systems, such as automatic target recognizers, are often fragile with respect to variations in the target's physical configuration. Using present-day technology, we are often embarrassed at late points in the development cycle as parameters of a key threat change, or new threats appear.

Observation 4: Automatic fusion is important since it will give a qualitative advantage to the US on future battlefields.

Our opponents on the battlefield have increasing access to such important military technologies as computers, data communications, accurate navigation systems, and cheap missiles. The integration of such threats into a meaningful military capability will be their primary

goal. Staying ahead of such threats will require us to radically improve our situation assessment capabilities for both manned and unmanned aircraft.

Data fusion technology will also be critical to the employment of precision weapons. In an era of powerful, cheap computers, even our least capable weapons can carry sophisticated onboard fusion algorithms and data links. Because of precision weapons, our opponents will find it attractive to hide. Camouflage, cover, and deception will be one of the very few ways they can evade more powerful sensors. They will also focus on hidden facilities and dispersion within their civilian population, knowing that our democracy considers it important to avoid civilian casualties. With precision weapons as the trademark of US Air Force operations, data fusion will be a necessary enabling technology.

Substantial progress must be made in automation if the full gain of future information architectures is to be realized. Onboard and offboard sensor data rates will increase by substantial amounts in the next century. It will not be possible to use this deluge of sensor data without new automated fusion systems that can automatically integrate multiple sources of onboard and offboard data.

Finally, data fusion is one way to improve an existing fleet in a cost constrained environment. As the Air Force enters the 21st century, many 20th century airframes will remain in its fleet. Inserting new technology into existing airframes will become an important business. Data fusion for situation assessment and targeting is one of the most cost effective insertions the Air Force can make.

Typical Fusion Applications

Fusion is an extremely broad subject. Example topics include:

- Multiple target tracking of moving air, space, ground or software objects
- Automatic target recognition based upon images, bit patterns, or time-varying signals
- Multiple *sensor* data integration, important to the process of unambiguously identifying individual objects
- Finding the position, location, and intent of someone attacking the military infosphere, and tracking the movement of their software objects through the network
- Natural language processing of text (perhaps derived from a speech recognition algorithm)

Fusion is a complex layered process, so much so that in recent years the research community has developed a standard reference model for describing its core functions. Figure 7 indicates some of the defining characteristics of this reference model, and points out areas that merit particular attention. Each layer and each issue highlighted applies equally well within the domains of imagery, position data, and objects moving through the infosphere.

Fusion Reference Model

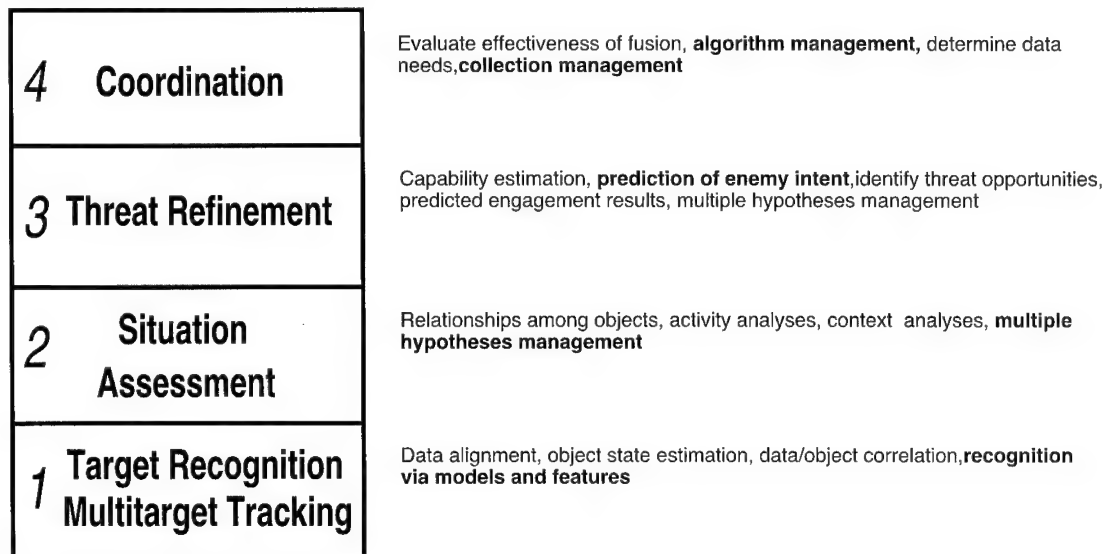


Figure 7. Multisensor fusion

Tracking Multiple Targets

Multitarget tracking is one of the primary requirements of the Air Force. Experience with large airborne radar aircraft has pointed to the utility of this function, particularly when the resulting information moves quickly to smaller attack aircraft. The problem of radar tracking of *complex closely spaced maneuvers by multiple targets* is representative of the issues involved. At the most fundamental level, the application involves one radar as it tracks multiple closely spaced targets. A basic issue is how to maintain track and identification through complex maneuvers. The algorithms for this application are decades old.⁹ The fundamental problem addressed in multitarget tracking is the difficult combinatorial considerations related to initiating and maintaining tracks.

Automatic Target Recognition Based Upon Images

Automatic target recognition based upon images recognizable by a human operator has been a key problem in both military and commercial applications. In the university research community and the commercial world, its primary application has been to robot vision. Numerous government development groups attempted to bring early forms of this work to a useful product. To date, none has been successful. Research support should continue for an important range of two-dimensional sensors: synthetic aperture radar, multispectral sensors, and electro-optic sensors. Progress in automatic target recognition from two-dimensional geospatial data is important because of the great volume of such data that modern sensors can provide. Early

9. They involve calculations based upon the assignment algorithm, 0-1 integer programming, Lagrangian relaxation, and other methods.

success is possible for the more modest goal of simply assisting human operators. The goal of complete automation remains an important but longer term prospect.

Integrating Multiple Sensors

More general forms of fusion involve multiple sensors: images, signals, and others. Fusion of radar data from multiple platforms involved in multitarget tracking would be particularly useful in air combat. The viewpoints of several aircraft could be combined into a common air picture. The identification component can be supplied from analysis of other signals using statistical pattern recognition, neural nets, or other means.

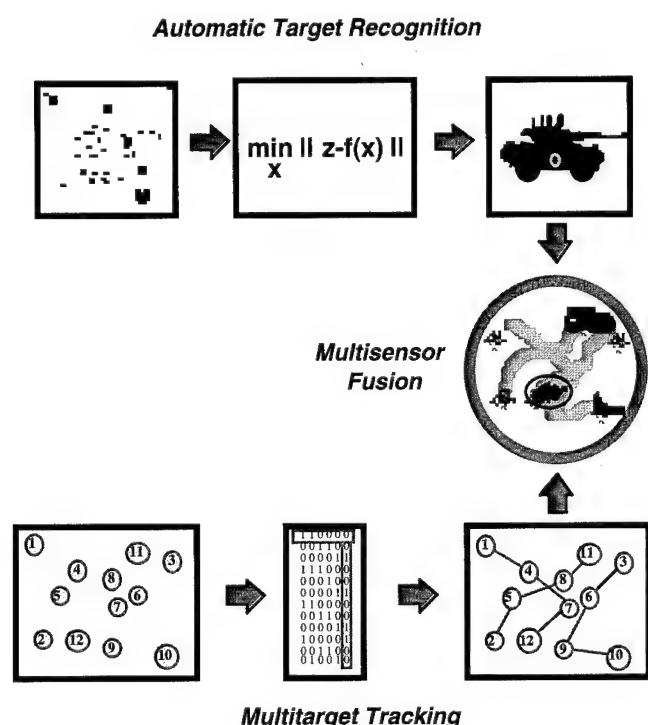


Figure 8. Core technologies for the fusion (more important denoted in bold)

The surveillance product is produced through an automated search among the likely ways data can fit together. Similar processes can be used for other sensor combinations. Figure 8 illustrates how this might come about when collecting two types of data: images and time varying position data. In this case, an automatic target recognizer (ATR) provides the identity of a key target, while a position tracker follows the time history of an entire collection of targets. In this illustration, two fusion sub-problems are solved first: one for ATR, and one for multitarget tracking. Final integration occurs at the object level at the conclusion of ATR processing.

Why Automatic Fusion Hasn't Worked Yet

What is the current state of the art in fusion systems?¹⁰ After two decades of research by groups in several different technical communities, automatic fusion remains an elusive goal. It has proven difficult even in the benign environment of a research

10. Level 1 functions are the most mature, with numerous algorithms tested on workstations with simulated and real data. Automatic target recognition systems today remain fragile with respect to variations in target parameters. Most Level 2 and 3 software is immature and fragile, due in part to heavy dependence on *a priori* expectations concerning target characteristics (for example the use of scripts). Expert reasoning engines are typically not integrated with the underlying Level 1 functions. Level 4 consists of mission planning, collection management, algorithm management, and response management. The mission planning and algorithm management layer is not mature. The typical system is manual, or uses a fixed algorithm execution path. Collection management has practical difficulties at the sensor level since there are typically few application program interfaces made available to system designers.

laboratory.¹¹ Robust solutions will require coordinated, well-funded, long term research programs. Attempts at a short term harvest of existing ideas from one or another of the various communities of interest will not produce broad solutions. Automation will require more than powerful algorithms. Attention must be paid to the clarification of surveillance architectures, sensor design, network communication systems, and simulation frameworks. Even if unique solutions are found for specific environments, the constant cat and mouse game of surveillance versus deception will require continuous evolution of our systems.

The difficulty of automatic fusion in conventional battlefield situations is replicated in the infosphere. In these applications, an added problem is the uncharted nature of the waters. We are in a fundamentally new environment, and tools that allow us to analyze information are only now emerging. Since the military infosphere intersects the private world in many ways, we will need to exercise great care that our tools are appropriate to their specific tasks.

We have found it hard to build manually guided data fusion software for workstations. We will find it even harder to design hands-off fusion software for maneuvering attack aircraft or satellites. Success in fully automated aircraft and satellite avionics fusion will depend upon a carefully coordinated effort managed by several Air Force laboratories over a long period.

Today's fusion systems, whether embedded or built upon an open standards workstation architecture, are primarily custom-built stand-alone software designs built to the unique needs of a particular project or military task. Underneath these seemingly different designs is a core of common functions. This commonality should be exploited in future designs that fit a broader range of applications.

As this monograph is written, most operational data fusion systems are designed to provide computer support for what is still a manual process. Although the theory of data fusion is well developed, most attempts at heavy automation have been too fragile (in an algorithmic sense) for actual battlefield applications. Even in the benign environment of workstation based intelligence analysis, fundamental improvements must be made before machine based fusion becomes a useful tool.

It now appears that serious improvement in the accuracy of automatic machine-based fusion will require careful integration of functional capabilities drawn from several different technical communities. For example, sensors are needed with broader spectral diversity, better resolution, more diverse viewing geometries, longer persistence, and higher observation rates. (These issues are described in detail in monographs by the Sensor Panel.)

Research Threads for Automatic Fusion

The following paragraphs describe some of the more important of research issues.

System Architecture

New, carefully integrated architectures are needed for Air Force information systems, both at a macro-level (Joint theater) and at a micro-level (onboard aircraft or other nodes).

11. Many of the successes of commercial vision systems have come as the result of carefully controlling lighting, target orientation, or other parts of the environment. It is precisely in these areas that military fusion systems are at a disadvantage.

They should provide rational processing and dataflows for knowledge integration and dissemination to all users. Many architectural issues involving fusion and command centers, sensors, and users have been traditionally decided by invocation of a security model, or by the dedicated requirements of specific users. Less importance has been attached to the possibility of incorrect or late results being transmitted to the tactical user. Other historical impediments include lack of adequate data links, and a military acquisition process that induces stovepipe system designs. As new technology and new policy provide solutions to these problems, reengineering of military fusion systems will be accomplished more effectively.

A careful architectural comparison reveals that many fusion or command and control systems have common components. As a result, systems built for aircraft, spacecraft, or ground nodes could have an important number of common algorithms and software objects. Proper development of architecture will permit greater utilization of shared components, leading to greater affordability.

Situation Awareness in the Military Infosphere¹²

The US military will increasingly operate its computer nets across a mixed military and civilian infrastructure.¹³ Security flaws exist in such systems, derived as they are from experimental research that has been quickly taken into everyday use. More potential flaws are introduced by the extension of networks to aircraft in flight. Threats to one part of the military infosphere might therefore affect the overall system as it becomes more densely interconnected through both wired and wireless links. Current military concerns are often focused on illegal entry into government ground-based computing systems. More disturbing is the issue of tampering with software objects in transit between secure systems, particularly in the wireless linkages required on the battlefield. The intent of such tampering might be to copy information contained within, or to insert some type of software munition.

Fusion research is important in the infosphere, since attacks against a network must often be *inferred* from uncertain data. Situations of this nature require analytical methods that can operate effectively even when multiple uncertain hypotheses must be maintained about the underlying situation. Many tools of fusion have been derived from general mathematical or psychological principles to deal with such problems. Some will be directly applicable to the infosphere. For most levels of the fusion model (see Figure 8), and in regard to sensors, new methods will be required.

Typical questions of concern are: Who is in our system? What are they doing now? What do they intend to do? Has a software object been tampered with in transit? Our sensors for detection are meager in comparison to the deluge of information pouring through the military infosphere. Software objects come and go in military networks in unimaginable numbers, without the explicit knowledge of their operators. Sensor design is difficult since attacks can be mounted from points of intersection with civilian open networks.

12. See also the monograph "Defensive Information Warfare in the 21st century."

13. Other monographs describe the type of robust distributed network communications that will couple various system elements regardless of their physical location, and permit knowledge delivery to the end user.

If and when the pace of computer evolution slows, it is possible that many of the vulnerabilities in open commercial systems can be closed. Today's rapid rate of development introduces vulnerabilities with each modification of software or hardware substrates.

Over time, it may also be possible to develop computing systems that are trusted by virtue of the design procedures used in the manufacture of software. Even then it will be important to understand the health of the military infosphere and the threats arrayed against it.

Fusion in Distributed Networks¹⁴

Fusion will take place in future years across distributed networks of sensors, computing servers, and platforms. Figure 9 indicates the environment that will be common in the next century.

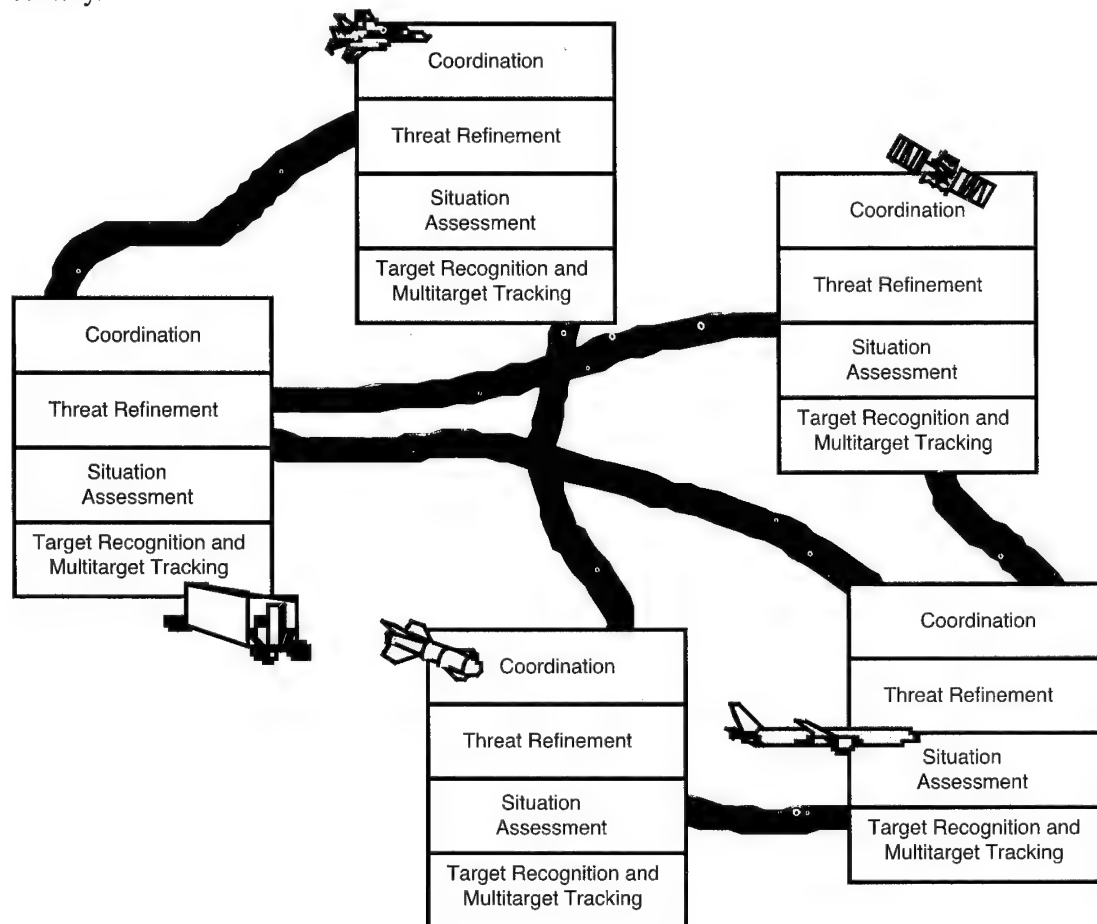


Figure 9. Fusion systems constructed to a common reference model, operating in concert across a computer communications network

14. See the Information Technology Panel's monographs for a discussion of scaleable and network-oriented computation.

There will be a continued evolution toward smarter sensors that draw more of the fusion process into the sensor system itself. Such an evolution may lead to lower bandwidth requirements throughout the data networks supporting the fusion process. This will make it possible to employ direct communication between sensor and shooter.

Current government research is developing the tools required to tightly integrate fusion systems across multiple nodes using parallel coordination languages. This approach will be particularly suitable in ground or other applications where communication links between processing nodes are relatively stable.

In more difficult environments (between aircraft and ground nodes) it may be advantageous to recast fusion algorithms on an agent-based substrate. This would represent a looser integration than parallel coordination languages, one that is more appropriate when communications can be delayed or interrupted for various reasons.

Symbol-Based Algorithms

The fundamental questions addressed in fusion overlap the artificial intelligence community in many ways. Among the more important overlaps is the following: how can common sense be integrated with numerical search algorithms to produce trusted systems for rapidly changing environments? Automation of the fusion process will depend in part upon our ability to integrate many separate tools (target models, search, and filtering algorithms) with very large amounts of domain-specific commonsense knowledge. Algorithm control (a Level 4 process in the fusion reference model) is cumbersome and fragile with traditional programming languages. As artificial intelligence technology continues its progress, reasoning systems with integrated truth maintenance should appear that are robust and practical for fusion applications.

In current systems, symbolic algorithms are used primarily on a stand-alone basis (often at Levels 2 or 3 of the reference model). Future systems will address the problem of integrating all levels of the fusion process with control algorithms drawn from artificial intelligence research.

Metrics and Models in the Fusion Process

This thread is closely aligned with the nature of specific sensor and target characteristics. It involves mathematical models and associated measurement interpretation metrics (signal processing, probability theory, model based vision and allied methods).

Other research is directed at the details of decisions made under uncertainty, which in strictly Bayesian terms becomes a lengthy calculation. Various theoretical approaches are used to alleviate this condition, and these detailed mathematical approaches will need continued support if automated fusion systems are to be built.

Search Methods

Intrinsically, data fusion is a search across uncertain data. Numerical searches and filtering techniques are required for its solution. Methods include statistical pattern recognition, neural networks, and combinatorial optimization. Relaxation methods are emerging for the decomposition of very large search processes. Tools that accelerate the search problems of fusion are still far from complete.

Planning and Resource Management

We need automated planning and scheduling systems for collection management. These systems couple sensors to the needs of end users and fusion algorithms. Early research in sensor management is currently underway within Air Force laboratories, and should be continued, particularly with a view towards its use on airborne platforms.

It will be important for sensor vendors to provide adequate software interfaces for external sensor commands at the outset. Application programming interfaces that permit external algorithms to easily couple to the sensor system are a necessary part of automatic fusion.

Security Models for Fusion

One of the major issues in the use of netted fusion systems concerns protection. Problems include those associated with the use of agents and parallel coordination languages across a distributed network where information attacks can occur.

Further development of the security and protection models applied to machine based fusion is needed. Current systems usually employ the Bell-LaPadula information disclosure model. This inhibits (downward) write and (upward) read of objects with different security labels. Other government agencies are pursuing multilevel network security research. The Air Force should also participate in this work.

Database Design

Trends toward higher volume sensor systems seem well established, making it necessary to develop the means to efficiently integrate data from very large distributed databases. Detailed and careful analysis of algorithms concerning synchronization, truth maintenance, garbage collection, and queuing delays will be required in such systems.

Commercial vendors will be able to supply much of the required database technology for workstation-based applications. However, specialized systems will be necessary for applications such as aircraft avionics.

Human Interfaces

Careful analysis is needed of the human-computer interface at the level of the end user. The key end users are commanders, analysts at workstations, and aircrews under stress in a battlefield environment. Each of these presents different issues to the interface designer.

The never ending games of camouflage, cover, and deception make it likely that fusion will many times not be able to produce a single unique opinion with high confidence. Therefore, systems will be needed that permit the presentation of multiple hypotheses to users under stress. For the airborne user, it will be particularly important to develop an approach that avoids information overload in the cockpit.

Simulation

Fusion systems are complex and require a significant amount of testing before use in operational environments. Space and airborne avionics applications are particularly stressing

for these systems since they must operate in a hands-off mode when embedded in fighter, bomber, or spacecraft. Fusion applications need a carefully thought out test approach, involving several levels of activity:

- Static workstation simulations with standardized data sets
- Dynamic workstation simulations
- Distributed simulations with realistic sensor data
- Hardware in the loop simulations

Since fusion devices will be employed in highly netted circumstances, the complexity of their operational environment should be represented. For example, in fighter applications new tactics might be employed that reflect a capability for rapid automatic fusion. The pilot community is justifiably skeptical of interposing complex software modules between pilots and their sensors. Laboratory demonstrations, with pilot in the loop, will be required to effectively evaluate and justify these new approaches to sensor data processing.

New Paradigms for Computation¹⁵

Computational complexity is often the fundamental issue facing Air Force information applications. For example, combinatorial optimization for multitarget tracking (a key problem in information fusion) is hard in the sense that cryptography is hard. Most Air Force algorithms implicitly respond to computational complexity with approximation, since optimal solutions are often impractical in a computational sense. Special designs based on conventional microelectronics (parallel processors, digital signal processors) have been used to accelerate computation in certain military applications.

However, a fundamentally new paradigm for hard problems is emerging: computation based upon deoxyribonucleic acid (DNA) molecules. It deserves to be nurtured by the Air Force. The DNA paradigm departs radically from current computer designs. It promises extraordinary benefits to the Air Force should it prove viable: it may be possible to build DNA based machines that operate at billions of tera-operations per second.

The research thread described below is oriented toward DNA computing, rather than other important paradigms (such as quantum computing). There are several reasons for this. First, such computers may be able to solve military problems of great interest to the Air Force. Second, the Air Force needs to develop a stronger capability in the biological sciences. Third, a simple DNA computing model has already been demonstrated in Len Adleman's USC laboratory. Fourth, Dick Lipton's theoretical work at Princeton suggests that DNA models support broader computational applications than the graph algorithm demonstrated by Adleman. (These include fusion, planning, and other problems of Air Force interest.) Last, studying DNA from the viewpoint of computer science may result in new tools for biologists. Whether or not computational applications of these models prove viable, the research will add to the base of biological understanding available to the Air Force and our nation.

15. The Air Force is grateful to Dick Lipton for his help in developing the thoughts in this section.

This work is very early research, and as such may best be supported under AFOSR sponsorship. Success in understanding DNA computations will require teams composed of both computer scientists and biochemists. A simple way to make this point is that DNA is not just a sequence of letters from a four letter biochemical alphabet. It has fine structure that plays an important role in computations. Computer scientists must become aware of this finer structure if they are to make important contributions.

DNA calculations are realized by performing feasible biochemical operations. Such operations may be simple (pouring two test tubes together), or complex (such as a polymerase chain reaction). A series of biochemical operations forms the basis for a single instruction multiple data (SIMD) computer. The state of this computer consists of a set of binary sequences encoded as DNA. Biochemical operations are carried out concurrently on each strand of DNA. Each strand executes the same computation, leading to a highly parallel SIMD computer. The minimum time required to complete a problem is likely to be measured in minutes or hours. The number of operations completed within these minutes or hours is so large that the number of DNA operations per unit of time dwarfs that of classical electronic computers.

There are several important research issues to resolve before DNA computation becomes a reality. These involve physical details of the calculations. DNA computations are based on processes that are neither perfect nor infinitely scaleable. Given these physical realities, what is the correct model for DNA computations? There are many operations that are possible to perform on DNA. What are the tradeoffs among them? There are subtle differences among the many feasible algorithms for computation that impact issues such as error resistance. What is the power of certain subsets of operations? Which operations can simulate others? What paths are available to speed up DNA computations? It may be possible to uncover new methods to make improvements to individual steps in DNA computations. Such improvements may dictate the ultimate viability of this paradigm.

Another question concerns the written notation for describing DNA computations. Computer science may be able to provide molecular biology a notation for complex operations on DNA. Currently, biochemists use graphics to describe operations on molecules. Such graphics are not a useful language for describing the operation of a computer. Building computer programs for simulation will require a new formal language for the various operations. Having such a notation raises many interesting questions. Is the notation powerful enough to describe most DNA operations? Does the notation have adequate formal properties? (For example, are certain questions about it decidable?)

Can DNA computations be made error tolerant, since they rely on physical processes that are not perfect? DNA computations are based on different physical processes than those in conventional electronic machines. Conventional machines must also be concerned with error. However, the inherent reliability of electronic switches is now so good that this is not the limiting factor in modern machines. What is the error tolerance of DNA computers? What is the cost of designing for better error resistance? What is the best method?

What can we do with DNA computers? There is an exciting difference between DNA computations and classical electronic ones. DNA machines are highly parallel, but relatively slow. Lipton refers to this unexplored part of computational space as that of "ultra parallel

computation" (UPC).¹⁶ Which problems belong to UPC? Long term surveillance and planning problems should be very well matched to DNA computation. Such problems are large and complex, but do not require response times that are measured in seconds.¹⁷ Other potential applications include cryptography and computer aided design

How can we simulate DNA-based computations? One of the lessons learned in the design and construction of electronic machines is the major role played by simulation. The same will be true in the area of DNA-based machines. Simulations can be performed on many levels.

Low level simulation of molecular dynamics will be computationally intensive and require powerful conventional machines. Such simulations may help answer a number of questions. For example, in some algorithms it is necessary to assume that particular DNA products are formed. The probability that they will form might be answered by such simulations.

Simulations at a higher level will be needed for algorithm design. For example, a simulator based upon some type of formal notation could be quite useful. Such a simulator would take as inputs simple rules that describe the computation. This would make biochemical programs much easier to describe, and increase the likelihood that computations will be specified correctly.

Conclusion

We have described a number of research threads that will, if followed over the long term, support the development of automated fusion supporting a variety of applications. These are:

- System architecture
- Situation awareness in the military infosphere
- Distributed networks and symbol based algorithms
- Metrics and models in the fusion process, and search methods
- Planning and resource management
- Security models for fusion
- Database design, human interfaces, and simulation
- New paradigms for computation

These research threads will require a long gestation period to produce the ultimate goal: fusion systems that automatically produce a very clear picture of large surveillance areas. Consistent programs with stable long term objectives are as important as funding levels.

An integrated objective architecture that spans the universe of surveillance systems employed by the Air Force should be one of the first steps. Other areas deserving immediate support include: prototype fusion systems developed for onboard applications, automatic target recognition, and techniques for distributed fusion. The area of DNA-based computation deserves early funding since years of research are needed to evaluate its potential.

16. R. Lipton, personal correspondence.

17. *Real-time* fusion is not in UPC because DNA computers need more than seconds to respond.

2.0 Defensive Information Warfare in the 21st Century

Dr. Larry Druffel

This paper assumes, and provides supporting motivation for, the proposition that an AF goal should be to achieve information dominance to enable the execution of its missions through unconstrained, but protected, use of cyberspace, including systems the AF does not control.

The author acknowledges the contribution of Tom Longstaff of the Software Engineering Institute to the paper, in particular to the discussion of malicious code and bounded vs. unbounded considerations.

The Importance of Protecting Cyberspace¹⁸

Cyberspace is essential to AF mission execution.

Successful execution of all AF missions will depend on AF ability to exploit information. Consistent with the trends in our society, use of information and the supporting information systems technology by the Air Force has become ubiquitous. The success of both combat systems and support systems relies on access and ability to process information. These capabilities, including people, information and supporting systems are geographically and organizationally distributed, reflecting the AF global mission. The Air Force depends on cyberspace. The information available to the commander is not local and is often not under his direct control, but it is accessible. This trend will continue or expand as the Air Force seeks to reduce its decision time to operate within an enemy decision cycle in order to achieve its goal of information dominance.

AF systems will include commercial products and use commercial infrastructure that the AF does not control.

Although there will always be a need for military unique capabilities, the AF simply cannot avoid using commercial products to ensure that the best technology is available in a timely and affordable manner. Likewise, although the AF will own and control some infrastructure, its anywhere/anytime mission requires that the AF also use commercial infrastructure such as communications, networks and information services that might be available.

Air Force must protect its cyberspace.

With this increasing dependence on information and on commercial applications and infrastructure, it is increasingly important that the AF protect its cyberspace. This challenge is much broader than the normal security considerations. Protection must not only include the AF assets, but also its access to commercial infrastructure and in some cases protect the infrastructure itself.

18. *Cyberspace*, "that consensually imagined universe where information reigns supreme," is synonymous with the phrase *infosphere* in our Panel's report.

Air Force must use commercial solutions for protection, but must not depend on those solutions solely.

Commercial owners of information will develop technology solutions to protect their interests. The AF should use those products and approaches but, since the risk tradeoffs may be different, should not depend on them solely. The AF should lead in the development and application of technology for protection. The Advanced Research Projects Agency has an exciting vision and is committing substantial funding in this area. The AF should work with ARPA to participate in the technology development and lead in the application of that technology.

While it may be desirable to embed protection mechanisms into systems, from both a communications perspective and a commercial products perspective, protection must be considered an overlay in much the same way that STU-3 is an overlay on the telephone system. The important point is that the protection mechanisms allow integration of available software products and access to local communications.

The AF cannot assume technical superiority.

Clearly the AF can depend on access to the best technology. However, so can potential adversaries. For the foreseeable future, the AF will rely more heavily on information than potential enemies will. In addition, the time it takes to acquire and field new technologies and train people in their use will put the AF at a disadvantage against a non-traditional adversary, terrorist, or protester. This is particularly true with respect to a technology that is changing as rapidly as information technology.

For less than a million dollars, a drug lord or terrorist group can acquire highly competent people, trained at the best US. universities, and equip them with the very latest technology. A small team of less than a dozen such people can easily conduct attacks on AF cyberspace, from outside the US., and often at no personal (physical, legal or social) risk. The average AF user will be powerless against such attacks and may not even recognize (s)he is being attacked. This does not imply that the AF will be at a net disadvantage with respect to all potential adversaries. On balance, we have more experience and greater access to technology. Our defensive systems can be better than their defensive systems and our offensive systems can be better than their offensive systems. But we must plan for the situation in which the systems we want to protect are not as sophisticated as an adversary's offensive capability. The implication of this is that the AF must plan for the possibility that an adversary can get inside our Observe, Orient, Decide, Act (OODA) loop.

The AF should train and equip information warriors.

Consequently, the AF should be prepared to train and equip highly competent teams of information warriors to monitor, detect and thwart such attacks. A sophisticated attack on AF systems will involve numerous preliminary probes to find vulnerabilities, test the ability to modify, leave backdoor traps for later entry, and assess the ability and kinds of responses to such actions. A trained team of information warriors with sophisticated monitoring capabilities could detect such probes, recognize patterns and help users take precautionary and preemptive defensive actions.

An early capability is evolving within the Internet. Small teams of highly trained people, called incident response teams, one variant of which is a Computer Emergency Response Teams (CERT), support various networks. The AF has a CERT team. In general these teams are more like volunteer fireman in that they provide a response service but have no authority to take preventive action.

Training specialists is not enough. Any AF person may be involved in the information war. As a user of information systems, each AF person is a potential target and must be trained to understand her/his role in protecting cyberspace.

The AF must make core systems impenetrable.

The AF must also analyze its core systems (such as those that provide coordinates to weapons) and ensure that they are impenetrable. Protection schemes involve assessment of risk. They often include assessment of the cost of penetration vs. the damage to the AF. For those core systems, such as the link between an aircraft and a weapon, AF will want to ensure that the communications is assured and the system fully protected.

In IW, the AF must be biased toward protection.

Since the AF places greater reliance on information technology than any potential adversary for the foreseeable future, information dominance will depend on the ability to protect its systems. Also, since the AF will make increasing use of commercial systems upon which much of the US infrastructure is also based, vulnerabilities in AF systems are likely to also be present in US communications, power, medical, financial and other systems. Potential adversaries will also be using the same technology and products. When vulnerabilities are discovered, there will be a natural tendency to keep that knowledge for offensive exploitation purposes. The process for making such decisions must include advocates for protection and the process must be biased toward protection.

The AF should consider providing leadership in protecting cyberspace.

No US Agency has clearly established a capability to protect the US infrastructure that increasingly depends on cyberspace. Many of the systems our society depends on are vulnerable. Our power, transportation, financial, airline control, individual airplane safety, and healthcare, to name just a few, are all systems that could be attacked.

The AF must develop a capability to protect its systems and its use of cyberspace. In doing so, it will be developing the technology and a capability to accept a broader role as a US champion in much the same way the AF has established itself as a champion for air and space.

The Dimensions of Cyberspace Protection

Unconstrained use of cyberspace implies protection in multiple dimensions.

These dimension include encryption, protection from malicious code such as viruses and worms, use of agents that cannot be corrupted as double agents, protection from intrusion, detection of viruses and trojan horses in incorporated software, operating system and infrastructure control, and mechanisms for recovery and alternate operation in the face of failure, disruption, and denial.

Both data and control must be protected

Data must be protected both from unauthorized disclosure and from corruption or loss.

Data is a sequence of bits to which meaning may be assigned. Data is generally well understood as consisting of the elements that are input to computers and the output produced by them. It is obvious that data must be protected from disclosure to an enemy. It is also important that it be protected from corruption or loss. Data represents both an enormous investment and an important resource that reflects the current state of many systems.

Control must be protected both from unauthorized users and from automated attacks.

Control refers to the process (computer program) that has execution authority of a computer system. Although many programs may be resident on a system and be invoked from a variety of levels, only one program has control of the execution of a given processor at any one time. Normally, the issues of control are managed by the operating system for resource allocation and performance reasons. For an intruding process to have an effect on a computer system, it must gain control. There are a variety of ways in which control may be passed to a program, including human action, local system action, or action by a remote process. Any of these methods may be used for legitimate purposes, but they may also be the means of relinquishing control to malicious code.

The distinction between data and control is becoming less clear in many modern systems.

Most traditional applications treat data only as input to the program. In such applications, data could be corrupted to produce inaccurate results, even crash the system if certain circumstances or sequences were not properly accommodated, but could not assume control. Increasingly, applications accommodate sequences of code as part of the data. This approach offers additional power, but it also introduces additional sources of risk. Programs such as Powerpoint, a popular application for creating viewgraph presentations, accepts code as input and will pass control to that code. In this way, malicious code can be introduced through data, providing yet another reason why data must be protected.

Another example of this notion of data being interpreted by the client is illustrated in the World Wide Web. The World Wide Web is a collection of programs that operate on files available on the Internet. Through a convenient point and click user interface, a human may look for information. The user interface is an interpretive browse. When the user clicks on a link, the page pointed to by that link is brought over to the user's machine. The interface program then interprets the information on that page. It may be asked to perform a variety of functions including displaying graphics. It is interpreting commands to run specific programs. The data could be structured to change the programs to be run and thereby have an unintended effect.

The World Wide Web also offers another kind of opportunity for confounding the user. Organizations place information that they wish to make available in a specified format. Each item for which they wish to make additional information available is provided a pointer. This pointer may be to similarly formatted data on the same computer or may be to another computer. If a malicious user gains unauthorized access to these files, (s)he can change the links and the unsuspecting user would follow the wrong trail - a wild goose chase through cyberspace.

Data and control must be protected in bounded and unbounded systems

A bounded system has common administrative control.

In a bounded system, the Air Force (or other DoD agent) has either central or distributed authority over all components of the system, and can conform to a defined set of policies and procedures. Isolated classified networks and layered encrypted networks are examples of bounded networks.

An unbounded system has no common administrative control.

The control and data takes place in an environment where the interconnected systems and sites are not under a common administrative control. In this case, the boundaries of such a system cannot be defined, since there is no central or distributed authority that “keeps track” of all the components of the unbounded system. The Internet—a non-hierarchical network of systems under local administrative control only—is one current example of an unbounded system.

At a bare minimum, a bounded system can be understood and all of its various parts identified. In an unbounded system, the various parts cannot be identified, their actions cannot be predicted, and there is no unified administrative control over the parts of the system. There are conventions that allow the parts of the Internet to work together, but there is no global administrative control to assure that these parts are behaving according to these conventions.

The architecture of secure, bounded systems is built upon the notion of a security policy with the existence and enforcement, or lack thereof, imposed by the exercise of administrative control. In contrast, an unbounded system can impose no global security policy. For instance, on the Internet today the backbone architecture is independent of security policy considerations

because there is no global administrative control on an unbounded system.

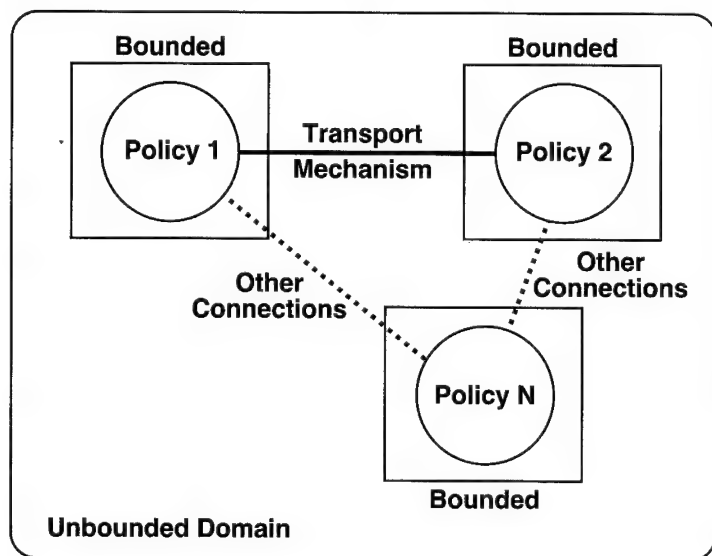


Figure 10 illustrates an unbounded domain consisting of a collection of bounded systems, where each bounded system is under separate administrative control. If each bounded system were completely disconnected from the other systems, it would be possible to fully characterize the security state of each system. Note that the notion of boundedness does not make any presumption about geographic constraints.

Figure 10. An unbounded domain viewed as a collection of bounded systems

It is not sufficient to focus only on the bounded systems. Protection for unbounded systems is also important because the AF needs the information derived from unbounded systems and needs to use unbounded systems as part of the infrastructure.

Threats and Countermeasures

There are a variety of threats and each threat requires its own countermeasure.

Electronic Warfare provides a more familiar analogy. There are a variety of threats and countermeasures. The data and control threats are different in bounded and unbounded systems. Likewise the responses to these threats are different. In addition, the maturity of the technology available to respond varies considerably. To a large extent the DoD has invested heavily in the technology and mechanisms to protect data, but has done very little to deal with control.

It is not possible to project all of the potential future threats. However, it is reasonable to begin by understanding the current threats and the countermeasures for those threats. Then as

	Threat	Countermeasure
Data/bounded	Disclosure	Data encryption Access control
	Loss of Integrity	Crypto Checksums
Data/unbounded	Disclosure	Authorization Authentication
	Disclosure in Transit	Data Encryption
	Integrity	Data Encryption
	Traffic Analysis	New Future Technology
Control/bounded	Trojan Horse	Strong Policy & Procedure
	Viruses	Limited Detection Prevention
	Internal excess of auth	Actg. & logging
Control/unbounded	Worms	Limited Detection Prevention
	Corrupted Agents	Docking Protocols
	Intrusions	User Proxy Firewalls

each new technology is introduced, the potential vulnerabilities of that technology can be assessed in the context of a deep understanding of these threats. While it may seem that the description of the threats and responses is irrelevant for the 2025 projection, threats introduced into new technology often follow the concepts used in previous technologies. There is some evidence that this is the case even though the mechanisms are often very different. The AF should not limit its thinking to a simple projection of known threats, but that is certainly a reasonable place to start. Table 2 captures many of the known or predictable threats and their possible countermeasures.

Table 2. Threats and Countermeasures

Data Threats - Bounded Systems

Disclosure

One of the principal reasons for creating a bounded system is to protect the data from disclosure to unauthorized people. This the most traditional concern of military intelligence and predates the use of computers. The typical response is to encrypt the data when it is stored. Unauthorized access to the data would be useless without the ability to decode.

Current capabilities for the prevention of disclosure include the use of both symmetric or asymmetric key encryption. The primary measure of the strength of encryption is in the time it takes to decrypt information without knowledge of the key. This time is related to the available performance and availability of computers used to "guess" or mathematically deduce the key. The constant increase in speed and availability of computers results in longer and more complicated key and encryption algorithms.

In the next 25-30 years it is likely that strong encryption algorithms will be available to the general population world-wide and it is equally likely that the ability to break current encryption techniques will be commonplace. At the same time, encryption technology is a commonly used technology to layer a bounded network on a larger unbounded network. Thus the government, and the AF in particular, should continue to develop strong encryption techniques for specific military use.

A second means of protecting data within a bounded system is by controlling access to the system so that only those who are authorized may access the data. These methods include physical identification schemes, passwords, and technology such as personal identification cards (like credit cards). This has traditionally depended on people and been labor intensive.

The technology for verifying that an individual is who (s)he claims to be is advancing rapidly. By 2025, a combination of voiceprint, use of uniquely coded identification cards, and possibly even human chemical analyses will be available to ensure that the person is who (s)he claims to be. It will not eliminate detection of an authorized user operating under duress or otherwise being "turned" to operate for contrary purposes.

Loss of Integrity.

A second consideration for data is that it not be changed by an unauthorized agent or process. In addition to preventing unauthorized access, techniques such as cryptographic checksums enable detection of changed data. They are also useful in the face of certain errors that may not be caused by a malicious actor.

Integrity has had little comparative attention as much of the research in security has focused on the prevention of disclosure. However, integrity will become more important to the AF mission as interactions with contractors and vendors migrates to the public-access networks. In this instance, the protection and integrity controls for all members of the public also benefits the AF. Older integrity models such the Biba integrity model and others may be adequate for use in bounded systems (Biba, K.J., 1975, "Integrity considerations for secure computer systems", Report MTR 3153, MITRE Corp.) The primary need for the development of integrity models is in unbounded systems and to protect against internal, unauthorized modification of critical data.

Data Threats - Unbounded Systems

Disclosure.

Disclosure of information to unauthorized parties is a distinct threat in unbounded systems. The threat of disclosure is similar to the case of bounded networks, but requires additional countermeasures as all end points may not be within a single administrative control.

An effective countermeasure is authentication that a packet appearing to be coming from a trusted source actually is doing so. In the link between trusted and untrusted domain, the AF should never let a bounded service be controlled by a program in an unbounded system.

Currently it is very difficult to prevent disclosure on unbounded networks. What is required is a national or international infrastructure that will allow third-party authentication and key management between parties. This would allow the AF and vendors, contractors, or private citizens to communicate using strong authentication and cryptographic protocols without prior arrangements. The use of ad-hoc technologies and partial solutions is the current state-of-the-art practice.

Unfortunately, the solution to this problem goes beyond technology. To promote the use of cryptographic technology throughout an unbounded system requires consensus with the method, strength, and exportability of the technology to be employed. Once agreed upon, the infrastructure must be funded and created to support the networks.

By 2025 it is likely that an infrastructure of some type will exist world-wide and it will be the challenge of the AF to work within this infrastructure as it evolves to effectively and securely communicate within the unbounded networks.

Disclosure during transit.

Disclosure of data while in transit from one bounded system to another bounded system through an unbounded system is at risk of disclosure. Such data is easily protected by encryption. Likewise integrity of the data can be protected by the same encryption techniques. See above for description of the appropriate technologies.

Traffic Analysis.

In traditional message-based communications systems, the Air Force has tried to block the inference of pending action by the analysis of traffic by an adversary. The nature of computer based networks with packet switching, reduces the vulnerability to such analysis. However, traffic analysis can be used to determine location of specific items. The traditional response of flooding a channel with artificial traffic is not an effective one because it only uses up available bandwidth and does not impede the analysis.

The prevention of traffic analysis is always at odds with the performance requirements of networks. Over the next 25-30 years it is likely that the use and prevention of traffic analysis will be addressed in the variety of new communication technologies that will arise during this time. The important point here is to address the security concerns (including traffic analysis) of any new communication technology prior to wide-spread deployment and use by the AF.

Control Threats

Threats to computer systems are based on system vulnerabilities.

Most systems are designed to perform desirable actions and not permit undesirable actions. Unfortunately, most systems have weaknesses that can be exploited to violate the system's intended behavior. These vulnerabilities may be exploited by direct human guided action or by programs, which are called malicious code.

Generally, control threats may be countered either by taking countermeasures into the initial engineering of the systems or by employing countermeasures upon the delivered and deployed systems. Currently, the development of systems employing these countermeasures have been guided by the DoD Orange Book requirements for multi-level secure systems. For Commercial Off the Shelf (COTS) and general-purpose systems, there has been little advance in trustworthy engineering, especially for systems designed to be deployed in an unbounded domain.

As the integration of COTS systems continues to dominate the character of AF systems over the next 25-30 years, the need for security engineering in these products will become even more critical. To accomplish this, it will be necessary to invest in new security engineering models, techniques, and products that take into account the unbounded network environment.

The terms defined in the following paragraphs offer one model of the types of threats. There are other models. These definitions are generally consistent with "Computers at Risk," a report of the National Academy.

Malicious code is a code sequence (program) which is not intended to be part of the operational system and does damage when it executes.

Malicious code is distinguished from erroneous code "bugs" that may be in a system. Bugs are code segments that were placed in the system intentionally to perform some function but, through some error on the part of the programmer, perform an unintended action. Malicious code on the other hand is inserted into the system either when it is built or inserted after it is put into operation for the express purpose of causing damage. There are a number of ways that damage can be caused: corruption of data, modification of action, creation of a vulnerability that can be exploited later, and crashing the system.

Protection from malicious code requires detection. Since detection of malicious code, in general is undecidable, cure is difficult to impossible. In practice, once a malicious code sequence is known, it can be detected. Once detected, it can be countered. In addition, protection without detection is possible using mechanisms such as limiting transitivity of trusted programs. (A transitivity limit of distance one would imply trusting a program but not trusting a program that had been modified by another program.)¹⁹

Current research in malicious code has focused on viruses and micro-computer platforms where there has traditionally been a lack of traditional security protections built into the operating system. While this will likely remain a threat for some time, before the year 2025 it is likely that

19. Cohen, F.B. "Defense-in-Depth against computer viruses." Computers and Security, Vol. II, No. 6, Oct 1992, pp 363-379.

all computer systems will employ multi-process and powerful computing techniques that will necessitate the use of security features to assure proper functionality.

However, the increased use of networked and distributed techniques will likely spur the development of distributed malicious code that will be difficult to counter using traditional host-based techniques. The current emphasis on firewall technology for network-based threats will not be adequate for many threats that will arise in a fully distributed environment. As a result, new protection technologies will have to be developed to maintain the security of a wide-spread distributed network.

One line of research that appears promising is the notion of mediators. The current line of research is to use an intelligent agent to intercept data base queries and to intercept the response. The agent would apply certain rules to filter the request and the response. If both were satisfied by the rules, the query would be completed. If it does not pass all the rules, it is routed to a human. The extension to full security would enable the evolution of a rich set of rules for managing the interface between bounded and unbounded systems.

Control Threats - Bounded Systems

A trojan horse is a program whose execution causes undesired side effects, usually unanticipated by the user.

A trojan horse is usually hidden within a larger program whose execution performs normally. A trojan horse is passive until its execution is triggered. When it executes, it can perform such undesirable actions as: disclose information to the outside, destroy data, or introduce a vulnerability into the system.

Protection against trojan horses is best provided by strong policy and procedures. A trojan horse must be inserted, either manually or automatically. Manual and automated policies for control of code, including change control, are essential to preventing introduction of trojan horses. Automated techniques include longitudinal algorithms, such as checksums, for detecting changes.

A virus is a self replicating trojan horse.

The biological analysis is appropriate - a virus can infect other programs. The distinguishing characteristic is that a virus is a trojan horse that copies itself, often attaching the copy to another program. If the virus propagates fast enough, it can have the effect of using up all the available processing time and clogging a network in addition to any other damage it causes.

Once a particular virus is known, its presence can generally be detected. In addition, limited detection is possible based on a virus' characteristic of replicating itself. Limited protection without detection is feasible by preventing specific actions from certain classes of programs.

Internal excess of authority is the assumption of system privileges by a program in excess of its rights.

Operating systems normally grant levels of privilege to programs. At the basic level, an operating system reserves for itself certain root privileges such as writing to certain areas of memory and controlling tables that establish privilege levels for applications programs. If a program attempts to accomplish some task such as writing to an unauthorized area of memory,

the operating system will normally block the action. A sophisticated user (or program) can often exploit an error in the operating system code to change the privileges allotted to it and thereby cause a variety of damages, including taking control from the operating system and even closing the system down. Note that this action is dependent on the existence of some vulnerability.

Control Threats - Unbounded Systems

A worm is a program that distributes itself in multiple copies within a system or across a distributed system.

A worm is much more autonomous than a trojan horse. It exploits system vulnerabilities to gain access to distributed systems. Whereas a trojan horse is passive until control is passed to it, a worm, once invoked, distributes itself by the positive action of exploiting a vulnerability in a target system, and passing control to the newly distributed worm.

An agent is a program that performs a specialized function such as monitoring activities, filtering data or seeking out data.

An agent is often considered benign and therefore trustworthy. Although some agents perform their function within the host machine, an agent may be "sent out" to perform its function on other machines. Unfortunately, a well intended agent that is sent out, can be corrupted so that if it should return, it can cause damage. This is a difficult situation since the system to which the agent is returning can no longer trust it.

Agents are powerful mechanisms but also introduce another type of vulnerability that has not been characterized or studied to the best of our knowledge. There is a current line of research to develop docking protocols which will require agents to "register" with the system to which they are visiting. Combined with encryption techniques, agents can probably be made safe for use both within bounded systems and for use between bounded systems across unbounded space.

Intrusions are unauthorized, human-directed access to computers.

Such unauthorized access is the result of some violation of policy, whether by an insider or an outsider. It may be the violation of an access policy or of a modification policy. It may be the violation of a human directed policy or of a policy that is controlled through automation.

When a human user interacts with a computer, (s)he is interacting with a program. The user may perform only those actions that the program allows. The program with which the user interacts may be on top of several layers of other programs. Through experimentation, the user may find that if (s)he provides some unexpected input, (s)he is passed through to some other program, even the operating system. (S)he may now perform whatever actions that program will allow, including access to data or modification of tables.

Malicious Code Summary

Figure 11 shows how these threats relate. This entire field is relatively new so that new types of threats may be developed which will require new characterization.

Within the next 25-30 years it is likely that the trend will move from host-based attacks to autonomous agent-like attacks that take advantage of the interconnection of systems with no

common administrative control. To counter these new threats, the AF will need to take a leadership role in prevention, detection, and recovery from automated network attacks.

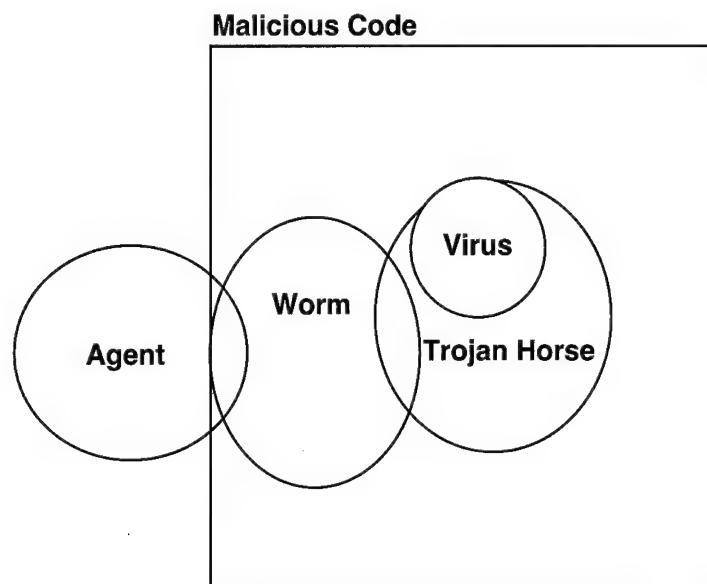


Figure 11. Relationships among threats

One trend that is likely to continue through the year 2025 is the expansion of the use of these threats by less traditional adversaries. For example, students may protest military operations through the disruption of distributed networks rather than a physical march outside an AF base. Likewise, a disgruntled employee can cause considerable disruption. The fact that the world will have access to the shared infrastructure means that an individual with motivation may be able to disrupt that infrastructure costing the AF significant time, effort, and perhaps even capability to successfully execute its mission. In addition, the expansion of the network technologies has led to more anonymous access such that the risk to an individual in performing these acts is minimized.

Recovery Technology

Despite the best protection mechanisms in automated systems, the potential always exists that some failure or disruption might occur. A single processor or communication link might fail or be denied, leaving no alternative for that element. However, other kinds of failure or disruption permit recovery.

In many cases involving human users of computing systems, the system gets into a state that is not in sync with what the user believes it is in. This can happen when a sequence of actions in which the human develops in her/his mind a model of what the computer is doing that is different from what the computer is actually doing. It can also happen due to some outside disruption such as a temporary or intermittent communications failure, action by a third party, or simply a mistake.

One example of this situation exists today. A PC user may have invoked a feature to access a remote UNIX system to acquire information via a database application. When a confusing sequence of characters appears on the screen, the user must determine which of the various systems in operation created the characters. The recovery action depends on whether it is the database application, UNIX, the communications handler, the operating system on the PC or the software controlling the remote access. A knowledgeable user can normally understand which system is creating the characters and respond appropriately to recover. As more effective user interfaces hide the underlying infrastructure software and less computer sophisticated users become more prevalent, users will be unable to recover from situations that should allow recovery.

A realistic example was posed during the AF/SAB study on integrated avionics. Using traditional federated systems, the pilot is able to build up a situational awareness based on the independent readings of a variety of sensors. When (s)he gets into overload, (s)he can focus attention on fewer sensor readings for which (s)he establishes priority. When the integrated systems begin to present a situational awareness to help with the overload, the system may present a state that is different from what (s)he expects because it has reached a state that is different from the mental model (s)he has developed. One easy remedy in that situation is to give the pilot a control which allows her/him to reset to some known earlier state even though that might be less complete than might be available.

It is essential that the AF pursue techniques that enable a user to recover from these situations. There are a number of well understood techniques and some research in this area. As commercial systems involve greater requirements for recovery, additional techniques will become available. However, the AF must ensure that available techniques are designed into the systems because they are generally not appliques that can be added as an afterthought.

Other Threats not Covered

Denial of Access

This paper does not address denial of access or disruption through such techniques as jamming, flooding the network and physical interference such as cutting communications lines.

Detection in Communications Link

This paper does not address vulnerabilities introduced by various communications links. For instance, cellular phones use a layer of protocols that communicate, in the clear, information about the user of the phone.

Embedded Trojan Horse

With the increasing reliance on software for supporting activities such as design, the potential exists for an adversary or other agent wishing to disrupt AF capabilities, to embed a trojan horse into software or even a chip that is used in a computer aided design system. As with the general case of a trojan horse, detection is not possible for an arbitrary segment of code.

This vulnerability will be exacerbated by increased use of commercial products (COTS) in defense systems. While this is a necessary and desirable trend, it means that AF will be incorporating software that was not developed under its control. The fact that the AF uses the software establishes the vendor as a target for those who might like to install a trojan horse. The

AF will need to work closely with those vendors and in parallel will need to develop techniques for checking the software.

Summary

This paper began with the assumption that an AF goal should be to achieve information dominance to enable the execution of its missions through unconstrained, but protected, use of cyberspace, including systems the AF does not control.

To achieve this goal, the paper draws the following conclusions:

- AF systems will include commercial products and use commercial infrastructure that the AF does not control.
- Successful execution of all AF missions will depend on ability to exploit information.
- AF must protect its cyberspace using commercial solutions where appropriate, but must not depend on those solutions solely.
- The technology will exist for AF to achieve the goal, but existence of the technology is not sufficient.
 - The technology must be used
 - Employment and training will be critical
- New technologies must be introduced aggressively but each new technology must be analyzed to understand and protect against the vulnerabilities it introduces.
- The AF cannot achieve information dominance without a preeminent ability to protect its information systems.
- The AF cannot expect to have technical superiority of its defensive IW systems with respect to the offensive IW capability of every adversary.
- The AF needs to train and nurture Information Warriors.
- The AF should train and equip to (a) monitor cyberspace activity that poses a potential threat to AF systems and (b) thwart a broad range of attacks.
- When an offensive activity identifies a vulnerability, a mature process must be in place to communicate that vulnerability to those engaged in protection.
- Since the US places greater reliance on information than potential adversaries, the US (both defense and civil) systems are at risk.
- No US Government Agency has established a credible capability to protect the US against hostile activity in cyberspace. The AF should consider filling this void and be an advocate for cyberspace defense at the same level it has for air and space.
- The AF should use its technology and capability to monitor cyberspace activity and thwart a broad range of attacks to protect US cyberspace interests.

Research Threads

The paper identifies a number of technology areas that the AF should pursue. These technologies must be pursued by monitoring and motivating commercial developments and standards, as well as pursuing defense unique capabilities:

- Encryption - including key agile technology
- Monitoring and intrusion detection techniques
- Techniques for designing trustworthy software
- Technology for detecting malicious code
- Firewall and mediator technology
- Docking protocols for accepting and managing software agents
- Recovery and resyncing techniques

Potential Payoff

The payoff to the AF includes:

- Ability to achieve information dominance of the battlefield
- Leadership in a critical area of defense to which the US is enormously vulnerable and which is devoid of champions

Acknowledgment

Dr. Tom Longstaff from the Trustworthy Systems Program at the Software Engineering Institute made several technical contributions to this paper, including the notions of bounded and unbounded systems and the characterization of malicious code.

3.0 Communications and Networking

Dr. Vincent Chan

With the disappearance of the USSR as the major strategic threat to the U.S., the most likely foreign crisis for the U.S. in the future will be regional (likely third world) conflicts that threaten our interests overseas. Since these conflicts can occur anywhere geographically, there is the need for a global defense network that can provide instant connectivity to surveillance/reconnaissance assets, rapid deployment forces and other military assets in a newly formed theater-of-operation, as well as in CONUS.

Applications

Future information infrastructure should have global reach and will be comprised of an interconnection of multiple, sometimes very disparate, communications systems or networks, some of which will be new and some which will include heritage systems in existence or planned to be deployed in the near future.

Concept (Tactical Theater Operations)

Components of these systems include: (1) satellite communications systems for the relay of very high data rate sensor-data, including downlinks; (2) military and commercial SATCOM systems (such as Milstar, DSCS, GBS, TDRSS, INMARSAT, etc.) for voice, video and data communications; (3) mobile SATCOM terminals for aircraft, ground forces and ships; and (4) a global reach ground network infrastructure that includes military and commercial networks. A special architecture will have to be developed for the proper internetting of these systems to provide an efficient infrastructure for data collection, voice, video and data traffic, intelligence data and map dissemination, precision-target and navigation information, messages providing classification/identification of friendly and enemy fixed, mobile and moving targets and command and control messages. This communication/network system should not impair mobility and should provide: (1) global coverage, as well as (2) coverage over any potential battle theater.

Figure 12. depicts the concept for a global network in support of tactical theater operations. Functionally, this information network must maintain connectivity with our forward assets, CONUS sites, other services and our allies. This requirement for connectivity is functionally shown in Figure 13. This network will include DoD developed systems as well as commercially purchased or leased systems. Since in a theater operation scenario, the geographic location of the theater may not be known well ahead of time, the defense network must not only provide instant connectivity to a sudden increase of users and user types but a surge in the capacity of the connections as well. Traditional DoD connectivities today are mostly by circuit switched voice service. In the future, data services will be more important and large number of users will have to be served by, in some cases, very precious resources. So sharing of resources via multiple random access of the network infrastructure will become an important aspect of the defense network. This would be a paradigm shift for the DoD and it behooves the Air Force to start this very important development and build up process by investing in the creation of the appropriate architecture.

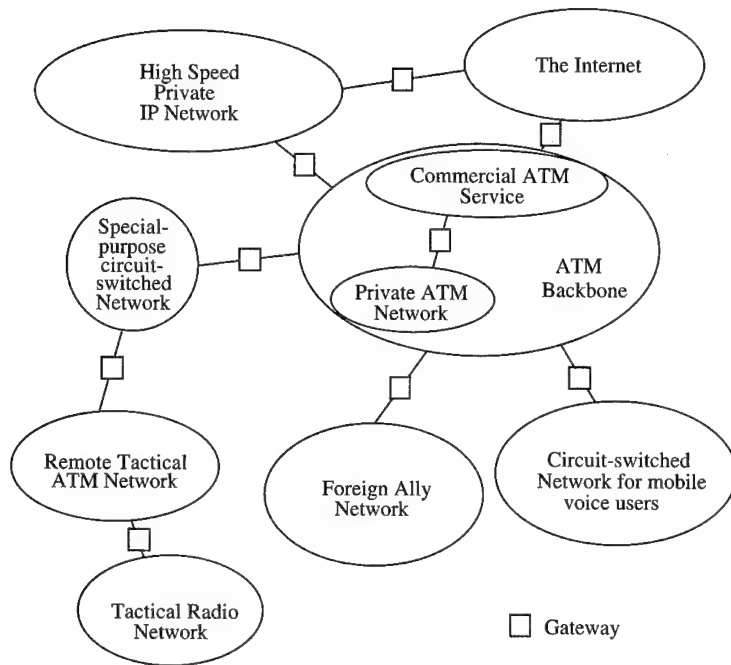


Figure 12.

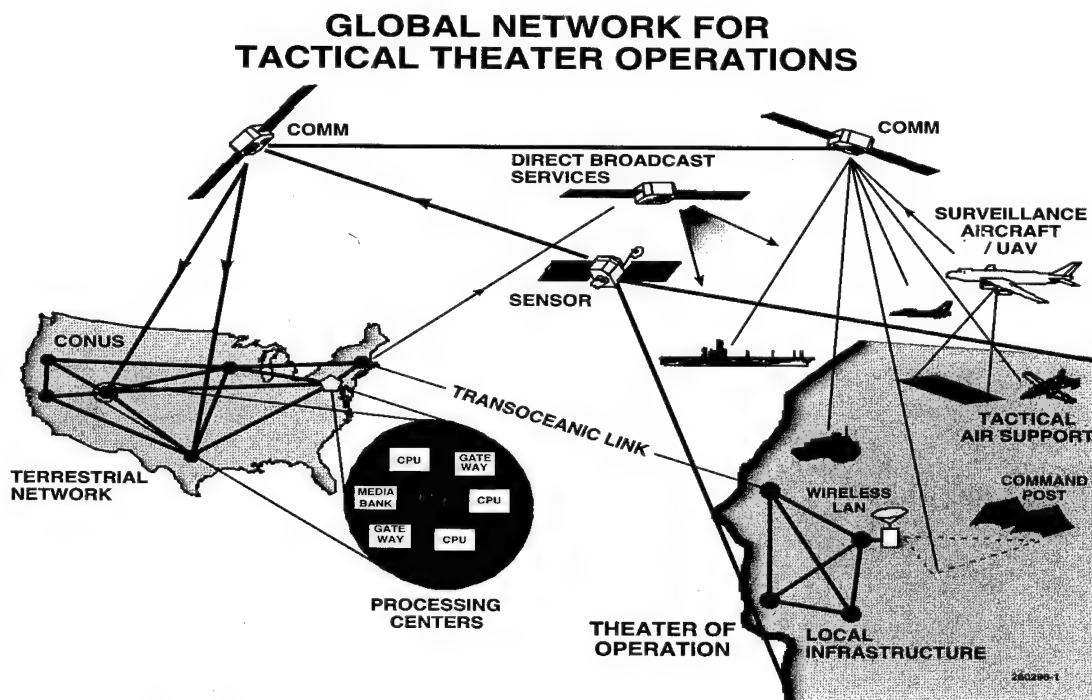


Figure 13. Global Networks for Tactical Theater Operations

Protected Core and Soft-Shell Network

With the rapid maturity of information and communication technologies world-wide, it is safe to assume that today's advance technologies will be available to our allies as well as our adversaries in the years beyond 2000. In fact the differential between US and foreign communications technologies will be closing with the rapid dissemination and deployment of commercial technologies, systems and services. Thus, it is imperative that the Air Force, in conjunction with other DoD partners, develop for its future a world-wide network with a protected, fully connected sub-network core that it can rely on for its war-fighting situations, even though part of the larger network (the soft-shell) can be denied due to electronic or physical attacks. In peacetime, the convenience of the larger capacity network can be used; but the war-fighting units must learn and practice to operate with the reduced capacities as well. Since highly protected communications services are expensive, high rate services may not be available to every user connected to the network. Thus, some units may have to operate based on protected message services only, rather than video or even voice connectivities.

While it is reasonable and pragmatic to assume the soft-shell outer network will be comprised of commercial as well as DoD developed systems, the protected inner core must have specially developed DoD systems and when commercial technologies or services are used, special DoD developed architectures must be employed to decrease the vulnerability of such systems. (An example of a more survivable ground network based on commercial fiber technology is one that uses multiple diversity paths albeit at increased expense). In addition, the critical irreducible information exchanges and connectivities for theater operations such as warfighting should be characterized and quantified. The core network must be designed to provide, at a minimum, those services even in the presence of a state-of-the-art physical and electronic threat. The network architecture must ensure the proper quality of service (QOS) is delivered to critical users of the network. Some of these QOSs are: deadlines for message delivery, time and location tacking, low error rates for data and low latency for interactive voice and video services. High QOS is hard to achieve with ad hoc network architectures. The Air Force together with its DoD partners should develop a totally rational architecture based on user requirements and what technologies can support. With current technologies, there will be some weak links (as discussed below). Possible system development paths to improve survivability should be identified. Since the threat level that will be experienced in a future conflict is highly dependent of the adversary's technological maturity, the DoD network architecture should be one that can sense its environment and adapt its connectivity and capacity accordingly.

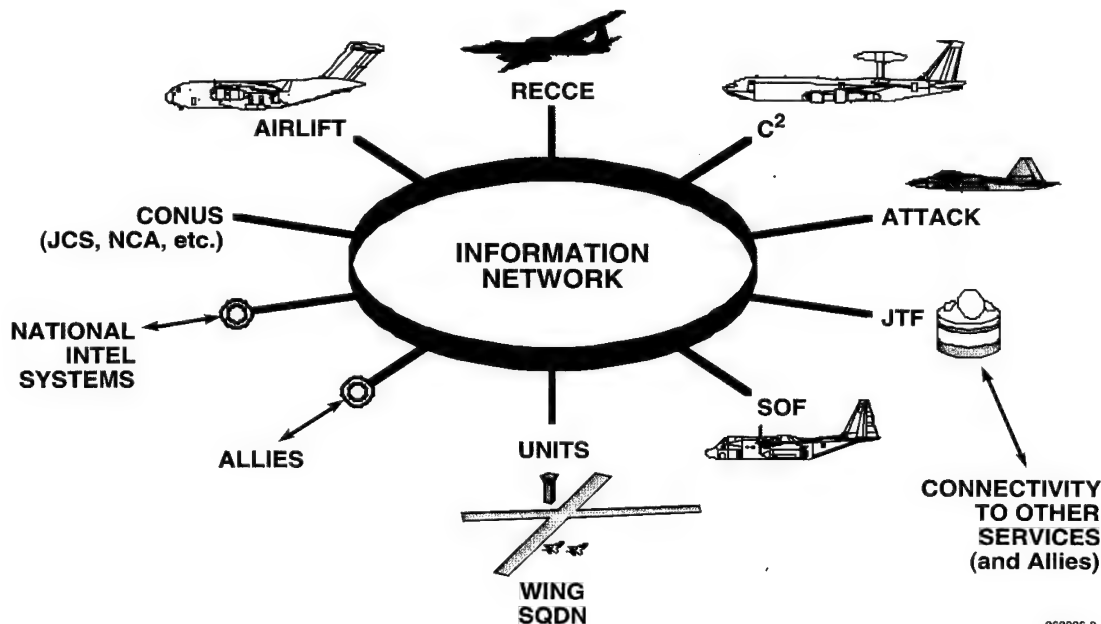
Service Types, Connectivities and Capacities

In future everyday Air Force operations and theater operations there will be significantly increased dependence on network services. Many of these services and connectivities will be new. It is probably useful to think about the necessary architecture by attempting to organize these services and connectivities, and their associated capacity requirements, into various classes (Figure 14 gives a graphic view of the necessary connectivities).

- *High Speed Trunks:* These will be used for data collection, dissemination, trunking of aggregated traffic (such as those between ATM switches), and large volume data broadcasts. These trunks most likely will be primarily fiber and in special cases via satellites for mobile connections and diversity protection. The data in

each trunk can be as high as 10's of Gbps. The connectivity requirement for this type of service consists of two types: (1) routine, slowly changing connections that make up the bulk of routine DoD usage globally (therefore a global extent), and (2) sudden surge of connections into a theater of operation at the beginning of conflicts (and therefore must be mobile and be capable of instant set-up).

- *Links Between Large Airborne Platforms and Command Posts /Control Centers:* Critical connectivities between airborne sensors (e.g. JSTARS, Rivet Joints, U2, etc.), airborne and ground based command/control centers must be maintained. This can be done by SATCOM or by some future in-air microwave networks. Types of services will include high rate data streams (can be as high as Gbps), voice circuits and multiple access datagram services.



260296-2

Figure 14. Connectivity Requirements for Future Air Force Communications Network

- *Broadcast Services from Satellites and Aircraft including UAVs:* Maps, intelligence products and situation awareness reports will be broadcast to the theater via SATCOM or airborne assets including UAV's, and direct from sensor aircraft such as JSTARS and Rivet Joint. The amount of data in the broadcast can easily reach 100 Mbps to 1 Gbps in the future, even with custom request data-pull from users. In the case of tailoring to specific user request for sending data in a broadcast, there should be at least a low rate return link from the user for acknowledgment of packets in the transport protocol. This return link is indispensable for critical message deliveries.

- *Connections between Fighters/Bombers and Command/Control Centers and Airborne Sensors:* This is the critical link by which the fighters and bombers can retain connectivity with the theater command and control infrastructure and also receive updates of situations and intel-products. This type of connection is typically very difficult to accommodate due to the limited space available on the aircraft for antennas, cost issues and the desire for the aircraft not to be detected via its transmitter emission. In this case, data service may be more important than voice service. Links of data rates up to Mbps can be required between airborne and ground entities even with significant data compression employed. In addition, there should be receivers for satellite or UAV broadcasts at 10's of Mbps and a low rate return link for acknowledgments if critical messages are to be sent via this mode. If on-board sensor data is to be shared among wingmen and also sent to theater rear, links originating from the fighters and bombers of Mbps class will be required to support such a mode of operation. Otherwise, lower rate data links will suffice.

There is a very important trade-off that the information infrastructure designer has to be aware of throughout the development process and that is: there is a significant trade between processing power and communication data rates. For example, more fusion and decisions at the sensors and the command centers will lower data rate requirements to the aircraft. Whereas for terrestrial fiber connections the cost of transport can be so low that a lot of compression and preprocessing may not be required. It is much too early to perform the trade at this point in time. The network designer should be conscious of this issue and the trade will evolve as the two technologies will in the next decade or so.

Satellite Communications

SATCOM is a critical element for providing connectivity to mobile and transportable military users in support of long range missions and theaters of operations.

General Perspectives

Current DoD SATCOM and commercial SATCOM can be utilized to provide connectivity. The DoD SATCOM systems operate at UHF (250 to 400 MHz) for low rate (up to 9.6 Kbps) unprotected communications to mobile users; at SHF (8/7 GHz) for low to high rate (up to 10+ Mbps) protected communications to fixed and transportable users; and at EHF (44/20 GHz) for low to medium rate (up to 2 Mbps) highly protected communications for mobile users. The services provided on commercial systems range from low rate services to mobile users at L-band to high rate services to fixed and transportable users at K-band. The key challenges which must be met to provide better SATCOM support to the tactical forces include inter-networking, increased capacity, and affordability. Inter-networking is required to bridge between different tactical SATCOM users via gateways between DoD and/or commercial satellites and into the terrestrial network. Increased capacities are needed for the military SATCOM links to support higher rates from mobile users and to provide increased global broadcast service (GBS) capabilities for information dissemination. Affordability will continue to be a challenge in an era of shrinking budgets and growing requirements.

There are major differences in the technologies and architectures of these military and commercial SATCOM systems. Furthermore, multiple administrative domains will be involved

in the construction and operation of the connected infrastructure, leading to a large degree of heterogeneity. These differences and the heterogeneous nature of the interconnected network lead to a number of technical issues which need to be resolved. These critical issues include internetwork gateway designs, network management and control, assurances of quality of service across subnetworks and network security and survivability. To create an affordable architecture is a challenging yet very important task. A substantial architectural design effort will have to be initiated in this area. A well thought out design with adaptivity and highly fluid interconnections can improve survivability, responsiveness and cost.

Protected and Unprotected Satellite Communication

Protected SATCOM achieves its effectiveness via a number of techniques: spread spectrum, anti-jam signal designs, on-board signal processing, spatial discrimination via shaped antenna beams and/or antenna processing (nulling). The Milstar EHF service is an example of a well protected SATCOM. With a combination of the mentioned techniques the Milstar system should be well protected into the 21st century, maybe with minor upgrades as technology develops in the next decade or so.

With the rapid advancement of commercial SATCOM technology and proliferation of commercial SATCOM services, it is reasonable to assume that SATCOM space and ground segment technologies will be widely available at a reasonable cost around the world at least by the turn of the century. At the lower frequencies (UHF, SHF), there will not be adequate bandwidth for band-spreading, and advanced adaptive antenna systems will be too large and costly to overcome commercially available jamming sources. Thus it should be assumed such services can be denied in the midst of a conflict with an adversary of moderate sophistication. Thus the Air Force might as well rely on commercial supply for these systems in the 21st century for cost reasons. However, these services and commercially supplied EHF can perfectly form the soft-shell communication network mentioned above, although multiple diversities of systems can decrease vulnerabilities some.

In the critical moments of a conflict, the Air Force must have reliable communication to its most important assets, such as sensors and airplanes. The protected core network should be designed to withstand reasonable projections of electronic threats. This system must have good anti-jam capability and low-probability of detection and interception. At EHF, 94 GHz and optical frequencies, there is enough bandwidth for spread spectrum or the frequencies are high enough to provide substantial protection via narrow beams or beam shaping. Again the Milstar system is a prime example of such a system, whereas there is little work done at 94 GHz and there have been many aborted unsuccessful efforts at optical frequencies. When the EHF frequencies become congested it is logical to move to these higher frequencies. Figure 15 attempts to put the many different DoD and commercial SATCOM systems in perspective.

Note that for world-wide coverage, these satellites must be interconnected via crosslinks or ground networks and gateways. When commercial technologies and/or services are used it is absolutely essential that such interconnection does not decrease the protection of such a system. Indiscriminate use of commercial fiber services, for example, may present unacceptable vulnerabilities to physical and electronic attacks. In this case, the commercial services should be considered unreliable and if needed a reliable architecture can be created over this unreliable

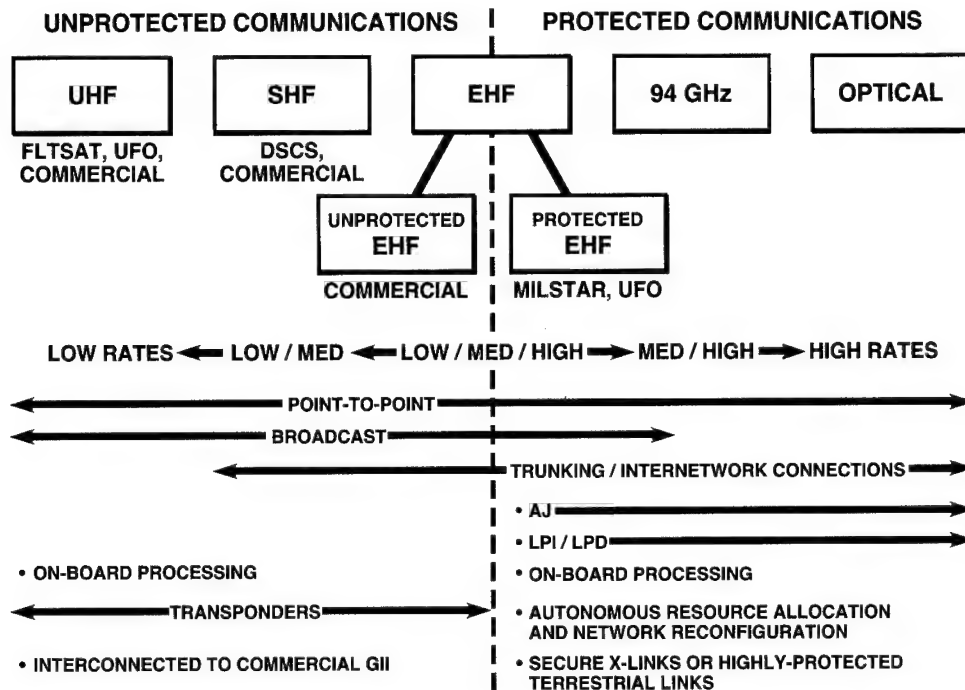


Figure 15. SATCOM Systems

substrate. This would require significant architectural development and higher deployment costs, which should be traded off against the costs of crosslinks.

EHF and Higher Frequency SATCOM for Aircraft

Many types of Air Force aircraft would function well with just protected critical message communication capability. Higher bandwidth voice and video are conveniences but probably not essential. This is fortunate since the cost of highly protected communications even at low rates is very high. EHF and higher frequency systems can provide anti-jam and low probability of detection and interception. Technology development in the next two decades should strive for low cost aircraft terminals. The enabling technologies include: solid state power generation, lightweight conformal phased array antennas and an architecture for sharing the channel medium efficiently for packet services with QOS peculiar to DoD, and specifically Air Force, applications.

One big stumbling block for the introduction of SATCOM into a small aircraft is the intrusiveness of the antenna, especially at high frequencies where antenna gain, LPI and AJ make their use inevitable. Current dish antennas are big, heavy and difficult and costly to integrate onto an aircraft. The enabling technology of the future will be the conformal phased array antenna that can be placed on the skin of the aircraft and the antenna beam is steered by electronically phasing the individual elements of the array. Present generations of phased array antennas use waveguide or free space propagation to feed the individual elements with their signals from a central processor. Unfortunately, these feed structures tend to be too thick for easy integration

onto the aircraft. Using fiber optics technology will make the feeds smaller and lighter. With this technology, the RF signals are modulated onto an optical carrier for transmission and converted back to microwave signals at the array elements. In an advanced form of this technology, optics can also be used to provide the processing and phase shifting functions. Research in this area has just begun, but it should be ready for deployment by the next millennium.

Intra-Flight (Air-to-Air) Communications

In addition to SATCOM to provide reach back and global connectivity for aircraft, there is also the need for intra-flight communications. Currently used UHF and planned EHF systems either have too low rates or their emissions can be readily detected at a distance and the aircraft located. Also some of these systems were designed before the rapid development of data networking and it is very difficult to interface these systems with other data networks. In most cases standard higher layer protocols cannot be simply applied. These problems will be further accentuated when the data rate requirements move up in the future from Kbps to Mbps. In a few links, such as those among UAVs, AWACS, Rivet Joints, Airborne Command Posts and other larger platforms the data rates requirements between two platforms can be as high as 100 Mbps. In the face of these new data flow trends, two techniques seem promising and should be pursued to provide high rate covert intra-flight and other aircraft to aircraft communications. These are 60+GHz and optical technologies.

Bandspredding can be used on an air-to-air data link operating with a modest transmitter (~2 mw). A communication link using this power could carry at least 200 Kbps using two inch apertures to a range of 20 miles if operating at 60 Ghz. The data rate would decrease with range squared or increase directly with transmitter power. An intercept detector at a range of 200 miles having a detector aperture of two feet would require an integration time of 200 seconds for a reliable detection (assuming that it is in a sidelobe). This is operationally impractical. If the link operates at the right frequency at 60 Ghz, additional path attenuation due to oxygen absorption would make the detector's task even more difficult, if not impossible (consequently, more communication power can be used to raise the data rate and/or range). The link needs a rapidly steerable or adaptive antenna due to its narrow beamwidths. Either a phased array or small dish can be used.

Optical links are also a possibility for covert air-to-air links. There have been a number of systems tried experimentally. They would have the advantage of narrow beams which are hard to detect. Also atmospheric absorption lines are available to limit detectability due to rapid power drop-off with distance, in which case broad beams (even omni) can be used.

Optical Space Laser Communications for High Speed Data Relay

Laser crosslinks offer the promise of very high data rate capability (>10 Gbps) coupled with very small package size (<100 lbs) for point-to-point links. Moreover, the high transmitter power (>2 W) and quantum limited optical receivers that now have been demonstrated in the laboratory, can be used to good advantage for lower rate crosslink applications where extremely small packages can now be built (e.g., under 40 lbs for 10 Mbps). Additionally, lasercom links are attractive for other applications such as UAV-to-UAV relay and UAV-to-satellite relay where high speed (300 Mbps) links can be closed with aperture size on the order of a few inches.

In the past, DoD and NASA have invested in several aborted unsuccessful programs in lasercom. The reasons for these failures can be attributed to the lack of understanding and elegant engineering solutions to critical areas of spatial acquisition and tracking of narrow optical beams, high power transmitter and sensitive receiver technology, thermal/mechanical/optical engineering of the space-borne hardware and overall system engineering. During the past few years, research and development have advanced to the point where these critical issues have been addressed and lasercom deployment in the 21st century is an achievable goal with continued development.

Terrestrial Networks

Commercial fiber-optic communications is undergoing a tremendous revolution in the 1990's. New installation of the latest generation of technology world-wide has increased capacities manyfold.

ATM/SONET Technology

In the years beyond 2000, the ubiquitous fiber transport will be SONET (Synchronous Optical Network) of various rate starting from OC-3 at 155 Mbps to OC-192 at 9.6 Gbps (usually by a factor of 4 in capacity at each increment). Since this internationally agreed upon standard will be wide spread, the DoD network should use the same standard whenever possible. For subnetworks that for one reason or another do not use this standard, proper interfaces should be implemented to bridge the networks seamlessly.

While SONET is a technology suitable for trunking, an emerging standard, Asynchronous Transfer Mode (ATM), can be used with SONET as connecting links between ATM switches for the support of heterogeneous users with very different requirements for rates and quality of services. The use of ATM technology in the military communications infrastructure should provide a number of significant benefits. The characteristics of ATM (efficient multiplexing and unified switching) should allow the deployment of a cost-effective network while providing a wide variety of services such as voice, video, and traditional data transfer. These are the same benefits expected by the commercial users of ATM technology. Furthermore, the fairly rapid pace of standardization of most aspects of ATM should allow equipment from different vendors to interoperate while the large commercial interest in ATM will ensure a large vendor base from which equipment may be procured. This equipment will be suitable for both private and public network applications. Finally, ATM is planned as the underlying "bitway" technology used by many domestic and foreign service providers, and many of these providers are expected to offer ATM user services at attractive prices.

All-Optical WDM Networks

SONET is a well established commercial standard for high speed optical transmission. Some long distance companies are now deploying point-to-point wavelength division multiplexing (WDM) in conjunction with SONET in order to further increase trunking capacity. Several research organizations around the world are now developing even higher capacity optical transmission and networking technology. Local area networks with 100 Gbps or more capacity and wide area network capacities in excess of 1 Tbps are envisioned.

One very active DoD/commercial research focus in the US is WDM network technology. These networks are capable of "all-optical" operations in that within the network there are no

optical-to-electrical transitions that may “bottleneck” the speed of the network or limit its versatility. Due to the characteristics of optical routing and switching, these networks are also rapidly reconfigurable. This is a very attractive property for rapid connectivity and capacity adaptation for recovery after link failure and sudden surge of traffic due to quickly changing situations. The rapid switching and routing property will be especially useful for the introduction of fast rerouting of the network as a form of ‘spatial path hopping’ to decrease the vulnerability against physical attack of the network. In this technique a connection between two users are constantly changing over many possible paths by some schedule protected by means of a key. This would make interception and total denial by cutting a single or a few links much more difficult. The technique can be one of several that can provide a ‘reliable network over an reliable substrate’. In this case the unreliability stem from the adversary. Several fundamental and enabling technology components have been developed including: fast tunable transmitters, fast tunable receivers, wavelength sensitive routing elements, multi-wavelength switches, and optical frequency converters. This area of research may lead to the next generation of high performance terrestrial networks and become the backbone of the DoD global network in the 21st century.

All-Optical TDM Networks

Future military communications, supported by an integrated global defense network, will benefit from the ability to rapidly process, fuse and disseminate large volumes of data with low latency. For example, processing centers and data archives located generally within the same geographic area will need a high performance local/metropolitan area network for communications. For this application, ultra-high-speed optical time-division multiplexed (TDM) systems, operating at single stream rate of 100 Gbps, offer important operating advantages over other multiplexing schemes. These advantages include increased “intelligence” within the network to perform dynamic routing which enables packet service (a service generally more suitable for computer data communications) and truly flexible bandwidth on demand with low delay.

Several key enabling technologies for these high performance networks must be first developed. For high speed transmissions, these systems will rely on nonlinear optical pulse propagation (solutions). Various laboratories around the world have demonstrated 100 Gbps propagation over 100 Km. In addition, short pulse sources, pico-second class optical clock recovery, optical buffering and optical switching for packet processing need to be fully developed together with the creation of a network architecture suitable for ultra-high speed low latency operations.

Wireless

In many terrestrial applications, it would be difficult to install instant wired connections. Thus the role of wireless networking will be very important. Currently there is substantial research and development in the commercial sector in the area of digital wireless mobile phone networks. Some of these developing systems are perfectly suitable for adoption to DoD usage. These include the various forms of Time-Division-Multiplexed (TDM) systems, Code-Division-Multiplexed (CDM) systems and some Frequency-Division-Multiplexed (FDM) systems. With high probability, direct application of such wireless technology may not be possible because either some military environment is different or the DoD network to be connected to needs

protocol conversion at a gateway. Thus a well thought out architecture is needed before such adoption.

Less well developed in the commercial sector is wireless data networking, particularly at burst rates of 10-100 Mbps. Interactive data transfers among ground units will be used in a variety of ways that go beyond traditional command and control voice networks. Examples include: transmission and discussions of maps, intelligence and weather data, medical status reports and automatic geolocation reporting and monitoring. In these modes of operations, the network will have to support packet service for efficient use of resources. The user traffic will be bursty and unscheduled, but continuous connectivity is almost always required, even though the user can be mobile. The wireless environment will be harsh for data networking even for commercial applications. In DoD applications, protection from at least some level of jamming and interception must be provided via spread spectrum and/or antenna shaping techniques. Systems should be designed to adapt to the environment in data rates, modulation characteristics and spatial directivity. Smart (agile) wireless networks that apply to DoD usage will not be developed in the near term for commercial systems. Thus architectural design and technology development should be initiated in DoD-specific areas.

Architectures

In support of the information needs of new warfighting concepts, non-traditional data connectivities need to be established. There are a significant number of developments of new hardware and system concepts to bring more of a data networking approach to military communication. However, there is still much to be done to develop individual systems and integrate them into a seamless network.

General Perspectives

Advantage can be taken of the explosive development of commercial products and systems, but there are a number of unique attributes of military communication in the theater grid that will require new solutions and their integration with key existing systems. Among these unique attributes are: physical and electronic survivability as in low-probability of detection and interception, anti-jam, data security and ultra-reliable message deliveries with hard deadlines.

The network architecture should have a hard core that is well protected against threats and a soft outer shell that can provide higher capacities in benign environments. The network management system should be able to adapt real-time as threats arise and increase protection (at the expense of capacity) and/or reconfigure to maintain critical connectivity. There are a few choices available today for the interconnection of disparate networks. The Internet interconnects many disparate networks in a flat amorphous hierarchy. But that system would have a problem with critical message delivery with hard deadlines. ATM (asynchronous transfer mode) has been proposed as the format for world-wide internetwork connection. In this role, it will have many benefits. However, there are real differences in the requirements of military and commercial communications systems. Furthermore, multiple administrative domains will be involved in the construction and operation of this infrastructure leading to a large degree of heterogeneity. These differences and the heterogeneous nature of the internetwork lead to a number of technical issues which need to be resolved.

Some Differences between the Military and Commercial Communications Environments

While most of the services that must be provided by a worldwide military network are in common with the commercial environment, some are different:

- There are few needs for on-demand, multi-gigabit per second flows in today's commercial environment.
- Generally, in the commercial environment, demand for service evolves slowly allowing time for reliable fiber optic channels to be installed in time to satisfy that demand. This is not always the case in the military environment where there may be insufficient time or resources to install high quality channels and switching of sufficient capacity. Even when there would be time to install sufficient capacity, finite resources or other requirements may make it difficult to satisfy demand. For example, communications subsystems which have good anti-jam capability or low probability of detection are often only capable of providing a low bit-rate service.
- When a resource, such as bandwidth, is scarce, one or more users may be denied service by the network. Commercial networks try to avoid such a situation by over configuring their networks to reduce the probability of blocking and by tracking usage to plan for the installation of additional capacity. Therefore, they rarely need to deal with the issue of dynamically adjusting the behavior of the network to allocate scarce resources to high priority users at the expense of pre-empting others.
- User mobility/roaming is an issue that is only beginning to be addressed in the commercial environment. This has long been a requirement in the military environment.
- Even in applications where mobility were not an issue, the lack of physically secure terrestrial or undersea fiber to every area of operations implies more inventive use of the same medium or the use of other types of channels, such as RF and free-space optical, to connect to the backbone. These links span many orders of magnitude in link speed as well as bit error rate and have very different characteristics that have to be accounted for in the network architecture.
- The level of sophistication of (and resources available to) adversaries in the military environment implies much more attention needs to be paid to all aspects of security in a military network. This includes both physical survivability and electronic survivability and security.
- Often, special purpose communication links are needed which must be operated near their margin limits implying the need for extreme efficiency in link usage.
- Finally, in times of crisis, some minimum level of connectivity (availability), service, and performance must be guaranteed. Network operations and allocation of resources may be different when operating in such a mode. For example there should be a high degree of dynamic adaptivity unlike commercial systems.

Significant architectural efforts are needed, early on, to recognize these differences and account for them in an Air Force/DoD network architecture.

Multiple Network Types, and Multiple Administrative Domains

Today's military communications infrastructure is composed of many systems in various stages of their life-cycle. Because there is a large investment in these systems (people, process, hardware and software), we must assume that these systems will continue to exist for some time to come. Therefore, despite the desirability of a homogeneous ATM communications infrastructure, this will not occur for a number of years. This implies a period where end-to-end communications will occur over a hybrid (ATM and non-ATM) infrastructure. This leads to a number of technical issues which must be resolved.

The most obvious way to apply ATM is in backbones. ATM is well suited to this and appropriate channels will most likely be available there. This may be done with a) government-owned links, b) links leased from commercial providers, c) use of an ATM service from one or more carriers, or d) some combination of the above. Each alternative potentially has different implications on the management, monitoring, security, and routing of the network. The general strategy for resolving many of these issues is to use some form of gateway.

Even in the heterogeneous internetwork model, we should not, in general, assume a simple model in which only one ATM network is traversed by a given connection (see Figure 5). So, although we would expect non-ATM links would be primarily used to access an ATM backbone, this would not be their only usage.

Another key issue in this heterogeneous internetwork (HI) environment is the existence of more than one administrative domain. Each network shown in Figure 4 may be administered by a different entity - each with its own local goals, processes, policies, and *capabilities*. This factor will lead to a major set of issues which will need to be resolved for a smoothly operating (and useful) HI.

In addition, since ATM is designed for high rate fiber links, there are a set of issues involving how ATM will behave (together with higher-layer protocols) when used on non-fiber links such as SATCOM and wireless. For example, ATM does not do well over channels with low reliability and has no provision to accommodate changing network topology as in the case of mobile systems. Significant network architecture developments will be required to deal properly with these issues.

Protocol Development for Data Communications

The DoD has only just begun to incorporate data networking into their mode of operations. Hardware and software for computer communications is readily available in the commercial sector. While some of these products readily apply to DoD systems such as leased commercial fibers, other DoD communication systems will require network protocol development (especially the higher layer protocols). In many cases, the underlying links (e.g. SATCOM, wireless) are not designed for the algorithms used in these higher layer protocols (such as TCP). The reason is that many of the current DoD communications systems have been designed for circuit switched voice applications instead of data services, much less random access datagram services. It would require modifications of the links themselves, or the higher layer (transport/

network layers) protocols or the insertion of adaptation layers in between to provide the proper interface characteristics. These modifications or additions should not be ad hoc but should be designed to operate gracefully within the world-wide DoD network. Thus an early definition of a network architectural framework is imperative.

Summary

The Air Force's information network of the future should have global reach for its normal day-to-day operations as well as a capability that can allow an instant surge of connectivity and capacity into a localized theater for mobile and fixed-site users. The latter capability is perhaps the most difficult and costly to provide but yet is a very critical and important tool for tactical theater operations.

This information infrastructure will be extensive in scale and comprised of both military developed systems and commercial systems at various stages of their life cycles. The network will serve many functions but yet can provide ubiquitous connectivity via interneting of multiple (often disparate) systems. The major services provided should include: (1) data relay from spaceborne and airborne sensors, (2) SATCOM and other relay (as in UAV) services to mobile and fixed platforms, (3) a high speed terrestrial network infrastructure that includes fiber and land wireless systems.

Traditional DoD communication systems today mostly provide circuit-switched voice services, with fewer systems that are designed specifically for data transmissions. Data services will be used more in future applications and the service requirements will be different than those of voice only systems. Because of the bursty and unscheduled nature of data traffic, sharing of resources via efficient multiple access schemes will become an important characteristics of this network.

For the terrestrial network, significant use of commercial fiber and the new generation of digital wireless technology will lower costs. With the advent of wavelength-division-multiplexed (WDM) fiber networks, capacities of multi-Gbps per link will be available and affordable. Since commercial networks may not have the necessary reliability, various DoD specific upgrades, such as, spatial diversity transmission, traffic masking etc. must be used for critical services. WDM networks, for example, can allow rapid reconfiguration with little service impact via all-optical switching. Commercial open standards should be used for seamless operations.

Perhaps the most critical and difficult link in the Air Force network of the future is the high speed (1 Mbps) two-way access link to the aircraft. This link must support fairly substantial rates with low probability of intercept (LPI), little vulnerability to jamming (AJ) and also be easy to integrate at low costs. The key technology in this area is light-weight conformal electronically steerable phase array antennas (likely optically fed) at EHF frequencies and above with significant amount of bandspreading of the waveforms used for LPI and AJ. This technology will have to be military driven, since commercial incentives for its development are not strong. While SATCOM will be the backbone of this system, a UAV intermediate relay can be a key element to lower terminal cost.

For the purpose of interconnection of networks, standard protocols should be used for interoperability and low development cost. However, current generations of higher layer protocols

that have been developed mostly for the fiber network, must be adapted to account for the less reliable and spatially changing links of mobile communications.

Since a significant amount of commercial assets will be used in the future Air Force network, the Air Force will have to deal with the vulnerability of these systems properly by creating a defense unique architecture that may use commercial transport as underlying substrates. The network should have a “hard core” that is well protected against various threats (physical or electronic) and a “soft-shell” that can provide higher/cheaper capacities in benign environments.

Research Threads for Communications and Networking

The AF should make maximum use of commercial technology and services. In addition, there are a number of defense-specific technologies that the AF should aggressively pursue:

- Low cost, LPI and AJ access links to airborne platforms at high rates (~1 Mbps), including optically-fed conformal phased array antenna technology, systems at new frequencies for more bandspreading, e.g. 94 GHz and 60 GHz(short range).
- High-rate optical crosslink technology for communication trunks and data relay.
- A defense-specific, reliable network architecture over unreliable substrates, creating an AF “hard-core/soft-shell” network.
- All-optical network (WDM/TDM) technologies for their potential in providing added survivability and security.

The Payoff to the AF Includes:

- A seamless world-wide network with the ability to deliver high-rate information in a timely manner to any user including airborne platforms.
- This network will adapt to various levels of threats and have the intelligence to provide critical connectivities even under the most severe attack.

4.0 Coordination, Planning, and Execution in an Information-Rich World

Dr. Harold W. Sorenson *and* Mr. Ronald D. Haggarty

Overview: What Can We Have?

Information systems technology, developing primarily in the commercial marketplace, has already achieved astonishing capabilities and there appears to be no end in sight for its continued growth. Successful application of information technology enables people from widely distributed geographic areas to work as an effective team, while simultaneously speeding up operations and reducing the number of people required to complete many diverse but necessary functions. As a result, businesses around the world are changing the way they operate to become more efficient, responsive, profitable and competitive. Within this commercially dominated, information-dependent world, the Air Force must evolve highly integrated, geographically distributed, collaborative information systems that work across both commercial and military information transport infrastructures to coordinate, plan, and execute the missions that it will be called upon to accomplish during the decades ahead. For convenience, the coordination, planning, and execution system described in this monograph shall be referred to as CPES.

In the future, the traditional coordination process through which combat planning, operations and related intelligence activities are accomplished will be replaced by virtual meetings of participants who, though geographically widely distributed, share common information data bases and are supported by an automatic real-time set of planning and scheduling services. The services will deal with operations options as they relate to logistic and support aspects of the engagement. For example, as decisions are made by the distributed participants, a three-dimensional “spreadsheet”-like calculator will execute all the support planning, scheduling and tasking actions (e.g., sensor tasking, air refueling, special EC support, airlift coordination, or emergency support) and issue the appropriate request and task order messages. The “spreadsheet” will update all related elements of the data bases as changes occur. This will contribute to the ability to wage continuous operations. Thus, it will be possible for new combatants to come upon the scene as the current ones pull back to refurbish their weapons—all in a smooth and continuous manner.

The traditional, centrally located “batch processing” method of command and control will have been replaced by a distributed, collaborative and real-time interactive process that utilizes automated computer-aided decision processes. Its key features will be flexibility, adaptability, and quick response. In the long-term, the information infrastructure and its automated decision support services will dramatically reduce the number of support staff required by decision makers at every command level. Using a sports analogy, it will be like shifting from football to soccer—no huddle with everyone on our side having a common view of the action. There will be a superb means of real-time communication between the command staff (the coaching staff), the shooters and sensors (the players), and the supporters (the trainers and equipment managers)—no time outs needed! Additionally, the shared view of the battle space will be augmented by covert means of communicating intentions between the shooters, an advantage not available on the soccer field!

These interactions will be facilitated through voice, including language translation/generation, and gesture understanding. It will allow dispersed individuals to work together in an "ordinary" manner, even while using languages in addition to English. The system will possess adaptive and intuitive human/computer interfaces that enable the user to access and utilize the distributed, heterogeneous data bases that underpin it.

In the world of 2025, processing, communication, sensing and positioning systems will provide widespread knowledge of everyone's location at precisely measured and synchronized times. Resources and objects will also be located and tracked with precision and this information will be available to all users of the system. Since any location can be characterized by its existing conditions (e.g., weather, man-made objects, terrain, ...), this information will be included in the data base. Thus, it is possible to envision people, vehicles, and resources being described in a geospatial reference grid that also indicates conditions at the location. Within this reference system, decision-makers and mission executors will have a temporal understanding of the situation that far exceeds any capabilities existing in 1995.

Planning will be accomplished in a continuous and interactive manner by drawing from information obtained from a variety of sources and sensors and contained in distributed, heterogeneous, object-oriented and relational databases. Participants can be geographically dispersed but brought together in "virtual meeting facilities". Planning tools that marry the methods of artificial intelligence and operations research will support the activity and facilitate the formulation of alternative courses of action. Then, simulation tools with high-definition video displays or 3-dimensional virtual reality presentations will be used to provide better temporal understanding of a situation and, thereby, aid the decision-makers in choosing the most appropriate course of action. Top-level direction will be transformed into specific mission plans at the appropriate organizational units and will be able to draw from the system all required information about the environment, particularly in the target area, and the vehicles, weapons, and support needs.

Mission executors will also have planning tools, including rehearsal capabilities. The simulation tools used to rehearse a specific mission will be available to all elements of the organization. When a plan is executed, information from the operational systems will be captured in the data bases of the CPES for rapid and reasoned assessments of mission effectiveness. The derived information will be available quickly to planners at all levels to enable them to press the appropriate actions in a near-continuous manner. The system capabilities should also incorporate on-line training. This will permit a higher quality of training with better feedback and less requirement for training personnel with associated reductions in cost.

In this environment, there will be a large fixed base of data and information. It is anticipated this information, suitably tailored to the situation, will be widely distributed and even carried by a user. Consequently, only the important changes that occur as the situation evolves will need to be communicated. By only communicating changes or immediate alert/warning messages, bandwidth requirements will be reduced substantially; there will be an automatic focus on changing events; and there will be an implicit autonomy for warriors when communications are disrupted.

The implementation of the CPES will be accomplished on a robust, highly-interconnected, flexible, and evolvable Military Information Infrastructure (MII). The MII will

use existing and evolving commercial components, standards, and specifications to transport military-specific information between designated locations. Since the commercial marketplace is defining and implementing the standards and specifications for object-oriented, open systems information infrastructures, the DoD and the Air Force must be active and aware participants with the national and international organizations that are doing the work.

The development of the MII and the CPES will benefit from research in several areas. The concepts that shape the vision of the system are becoming available now. The maturity, robustness, and performance of many of the tools leaves something to be desired, but research on some current limitations should produce substantial improvements during the next few years. It is anticipated that there will be very powerful capabilities by the year 2025. The system needs to have an architecture that accommodates realistic growth in capability. The complexity and the related dimensionality of the system defines an overarching concern in all aspects of the development and imposes a particularly important constraint on the definition and design of the system architecture.

There is one major threat to the concept. An integrated system of the type that is envisioned must be secure by detecting attacks and responding as appropriate. Certainly, the system must be designed to degrade gracefully and must provide assured access to information that has maximal integrity with minimal chance of disruption, spoofing, or disinformation. The topic of information protection is a fundamentally important consideration for the envisioned system. The virtual environment provided by the MII feeds into the C⁴I functions (i.e., CPES) which supports the organization and its ability to conduct operations. The fact that the loss of information security in MII or CPES will have a direct impact on the ability of a commander to conduct operations is depicted in Figure 17.

Think Big

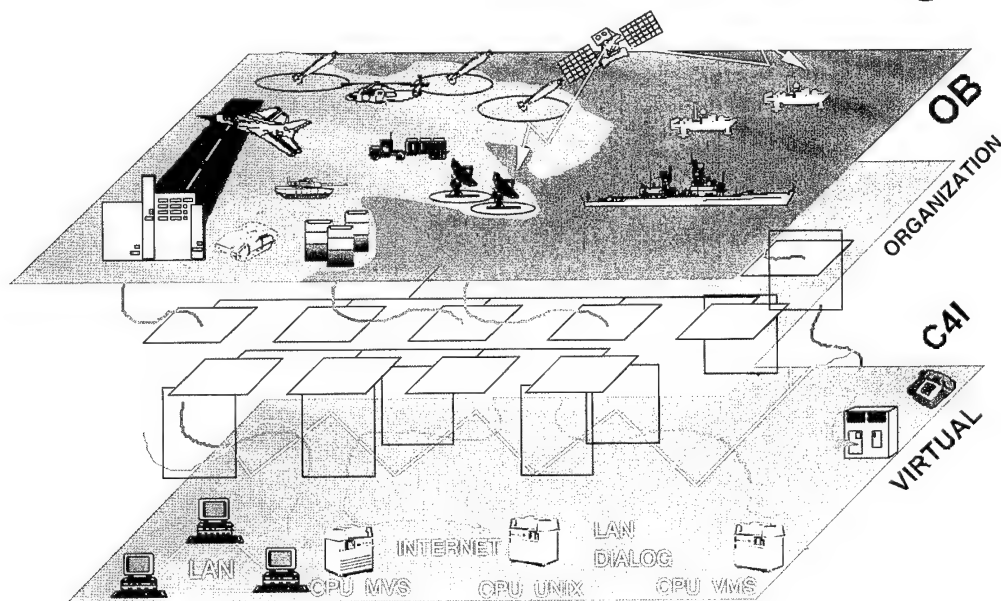


Figure 17, C⁴I Security Is Critical to Operations

Information System Enablers

Information systems technology will enable the realization of a coordination, planning, and execution system that allows continuous, simultaneous, horizontal and vertical interaction throughout the organization. One can envision the system as a "utility" into which any individual in the organization can "plug" an "appliance" to gain the information that will enable them to accomplish their mission/task. The utility will connect the highest command levels of the organization (i.e., commanders) to the individuals charged with accomplishing specific tasks (e.g., shooters, sensors, logisticians, maintainers). Underpinning the top to bottom command relationship between the commander-operator are the lateral and parallel commander-sensor/logistician/maintainer relationships that provide supporting resources that enable the shooter to execute his mission/task effectively.

There are several systems and technologies that must be available to realize the coordination system that is postulated below.

Computers: The reduction in feature size is projected to continue at an exponential rate for an extended period. Thus, one can envision the availability of computing capability in all endeavors with enormous throughput for computationally intensive activities. The only computational limit may be in human imagination and in the willingness to change the paradigms which have been utilized in the past.

Memory and Storage: Memory and storage devices of all types continue to grow in capability, matching the growth of computer speed and throughput. This technology encompasses the development of database concepts that support massive amounts of data and information. Concern changes from the technologies to the integrity and security of the information and to the methods for extracting appropriate information from the system.

Displays: Increasing computational power enables the consideration of displays that beggar our current capabilities. Flat panel displays with $(n,000) \times (n,000)$ pixels are possible. HDTV, "virtual reality", and dynamic holography promise to provide visual interfaces that enable "virtual meetings" and "virtual situation displays" that support human interaction and understanding in substantial and meaningful ways.

Communications: The communication capability envisioned for the future enables one to assume that any two points on the globe can be connected with high band-width links. The combination of fiber optic and wireless systems will permit robust connections that are already being manifested in commercially available products. While there may be choke points in the system (e.g., fighters), there should be sufficient band width to support most of the needs of the DoD. It is worth noting that the increased demand for video and imagery may continue to cause the communication system to be stressed. Thus, there will probably always be a requirement to conserve bandwidth by minimizing the information to be transmitted to that which is really needed. There may be problems in having militarily-reserved frequency bands, but these issues must be worked beginning now if command and control elements are to support national security objectives with commercially-developed information technologies and infrastructure.

Positioning: GPS and its successors will provide the capability of having a universally-accurate and available time standard that enables time alignment between geographically disparate activities. Everyone will know their location to within fractions of meters. Then, the

communication systems of the period will inform any other person or activity of this position information. Thus, one can postulate that in 2025, the organization will know “where everyone is at all times and in all places.” Further, there will be a complete description of all conditions at a specific location to assist in achieving the greatest possible situational awareness. Any vulnerabilities of GPS and its successors to jamming will have to be considered in the overall system design.

With the computer, memory, display, communications, and positioning capabilities, the traditional compartmentation of “command, control, communications, computers, and intelligence” (C⁴I) will undergo a major revolution. The C⁴I function must become focused on providing the infrastructure, or information utility, that permits the “plug and play” environment within which the coordination, planning and execution functions can be accomplished. Implicit in this discussion is the dependence of the system on the utilization of a broad array of *sophisticated software products*. The classes of these products that are fundamental to the system concept are defined and described, briefly, below. For this discussion, the information utility that constitutes the infrastructure for the new C⁴I system will be referred to as the Military Information Infrastructure (MII).

The Military Information Infrastructure

The military information infrastructure (MII) must have several key features that can be viewed from several complementary perspectives.

Different Views of the MII

Adaptability, Flexibility, and Timeliness: It is not realistic to consider building a rigid and highly detailed MII architecture that incorporates all possible alternatives if, for no other reason than the components, standards, and specifications that underpin the MII will be determined by commercial marketplace decisions. Therefore, the MII must be able to adapt to unforeseen circumstances, whether induced by the military or by the commercial world.

The commercial market place is driving the information systems of the present and future. The military is a relatively small market force that can try to influence commercial developments, but will follow more frequently than it will lead. However, the commercial world has very similar needs for information and similar coordination challenges; so the military needs to be knowledgeable and proactive with commercial developers about the tools with which it will be provided. By being involved and by making solid technical contributions, the DoD can still be influential in the process.

In this commercially-dominated environment there is an emerging need for a new or strengthened role for the technical community within the Air Force. *It becomes more important to learn to use existing and emerging capabilities in the domain of military applications than it is to develop the capabilities themselves.* However, shortfalls in the existing and emerging products must be identified. These assessments can serve to focus emphasis on important research topics, either for the military or for commercial industry. This point will be discussed further in later sections.

The ability of the military to respond quickly and effectively to a wide variety of crises that may arise concurrently is of paramount importance. The requirement for rapid response

into areas having a high potential for armed conflicts with uncertain outcomes may distinguish the military from most, if not all, civilian situations. Thus, a fundamental consideration in the MII is the simultaneous performance of the system across a wide range of missions at numerous global locations having variable capabilities for the indigenous support of operations. This means that there must be, in addition to being flexible and adaptable, a strong emphasis on system-wide performance. Tools and agents that cannot meet the timelines of a situation will have to be improved or replaced. Thus, another thrust of the military's technical community will be to develop specific tools that support the time-critical missions/tasks faced by the DoD.

"Push" and "Pull" Architectures: The need for information takes a variety of forms. In many cases, there is a large community that needs to have a specific piece of information. This information needs to be broadcast, or "pushed", so that it is available to anyone, possibly undefined, who needs it.

But not all situations are accommodated most aptly by a broadcast. If everything is pushed, individuals may suffer information overload and their ability to perform is degraded rather than enhanced. In fact, there is a large amount of information that is location, situation, or function-specific that has limited utility for a broad community. Information filters that limit the data accepted by a site provides some control over the amount of information that is received. However, there are many instances in which the user will be served better if he can "pull" desired information from appropriate data bases in a timely and assured manner.

The MII must be structured to accommodate both push and pull requirements. The push of information can have many advantages. For example, it does not require a attacking aircraft to radiate and, thereby, disclose information about his location to the enemy. In either case, there are fundamental advantages and disadvantages and these considerations must be included in defining the architecture for the system. The general topic of information management constitutes a fundamental challenge for this or any other large-scale information system.

Integrity: The information must be accurate, timely, and available. If a user has no confidence in the information, the system will have failed its mission, and will not be used. Accordingly, considerable attention must be given to the quality of information, including confidence estimates, whenever possible, in databases or in broadcasts.

Security: The information that is communicated must be assured in several dimensions. Broadcast information must be protected against jamming or interference that jeopardizes the link or the quality of information. Information extracted from databases must be unaffected by any transmission problems caused by enemy actions. Furthermore, the information that is received must be validated; no spoofing or deception from an enemy can be tolerated.

To emphasize, the MII and its operation must be "invulnerable" to the hostile acts of any enemy in the sense that it must be able to detect attacks, reconfigure, and operate in a degraded mode.. The integrity and security of the information in the MII has to be assured or the entire concept must be reexamined. It is asserted that the advantages of the MII merit the implementation of the vision. But *information warfare* considerations need to drive the development of the MII. A scheme for actively *managing* security must be developed in parallel with the development of the system.

Coordination, Planning and Execution Characteristics: The MII must support three characteristics that define the overall coordination, planning and execution function.

Resources: The databases that comprise the core of the coordination system are many and varied in nature. These databases contain information that relates to sensors, intelligence sources, geodesy and mapping, vehicles, weapons, and support of all types. Every function performed by the military has need for data and information. The MII will accommodate all of these needs. The massive database system of systems that results places unique demands on the methods for maintaining, accessing, interrogating, and retrieving the information contained throughout the MII.

Actions: The resources are used to achieve global situational awareness. Awareness is hollow unless it permits timely and effective actions. Thus, information must be available on demand to the commanders who direct actions and to the sensors and shooters who execute them. The MII must support the planning process and the direction must be communicated and executed by the shooters. The directions and the manner in which the execution is accomplished become part of the database as well.

The coordination, planning, and execution system is the centerpiece of the banquet table of information provided by the MII. In general, the CPES supports activities at all levels of the hierarchy. It represents the mechanism by which the users of the system interact with the MII to accomplish their goals and objectives. Because of its importance, the planning system is discussed in some detail in a later section.

Outcomes: The result of the actions taken by commanders and shooters must be measured and assessed, with the information being incorporated into the system. The “battle damage assessment” (BDA) is accomplished using resources controlled by the operation of the MII. The feedback from the BDA closes the loop on the commander’s decisions and shooter’s actions. As such, it is another key feature of the planning system that must be accommodated in a timely and flexible manner.

A Concept for Data Management in the MII

The concatenation of Resources, Actions, and Outcomes introduces the paradigm that is fundamental to the coordination, planning, and execution system. The importance of these three characteristics is captured by envisioning the linkages and couplings that are implicit. For example, a commander makes a decision to send a flight of F-16s against a ground target. Before they can be sent, the availability of specific aircraft, the appropriate weapons, the crew, the fuel, etc., must be established and the facts must be factored into the plan (hopefully, as automatically as possible). Before the launch, events may occur that force the plan to be changed. After the attack, results, including damage to the enemy as well as our own situation, must be introduced into the databases.

Many of the elements of the databases are tightly linked. The coordination, planning, and execution system needs to be aware of these linkages so that all relevant elements can be modified appropriately, automatically, and quickly. The model of this feature can be captured in the context of current computer tools by representing the desired actions as a “three-dimensional spread

sheet.” The basic variables are provided through the resource database. The other two dimensions are defined in terms of the planning/action activities and of the BDA process and results.

The paradigm is intended to provide the impression that when a cell in the 3-D spread sheet is changed, changes appear automatically in every related cell. Thus, the updates from new information are incorporated with a single entry, no matter where it is located in this three-dimensional space, and the fidelity of the entire database system is retained.

To implement the 3-D spread sheet, there are many hurdles to be surmounted. The biggest challenge may be posed by the “dimensionality” and complexity of the problem. This speaks to the need to define an architecture that uses well-defined and reasonably focused objects that have minimal coupling to other objects. This is only one aspect of the architectural requirements for the system. Figure 18 depicts the different realms that must be considered when we refer to “architectures” and all must be considered as the MII and the CPES are designed.

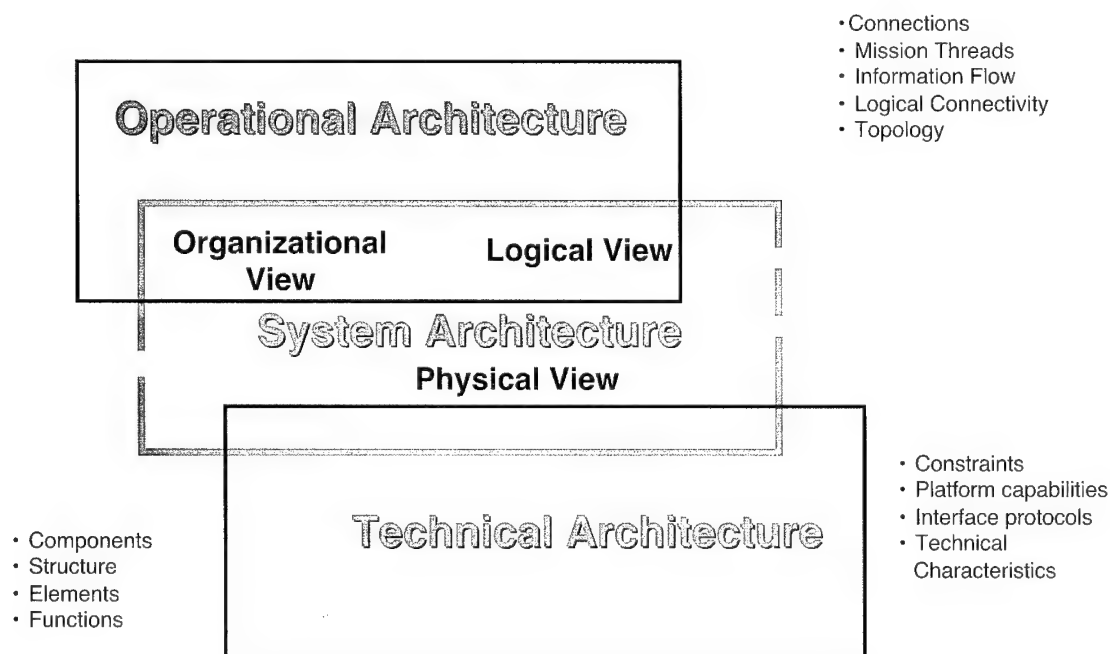


Figure 18. The Many Faces of Architectures

Coupling among data elements is an obvious type of linkage that must be controlled by the 3-D spread sheet. A very different type of coupling that must be accommodated comes from the change and updates that will occur in the commercial products that are used to build the system. As we experience regularly, new versions of software products are not always compatible with older versions. Software that is widely used in the system may exhibit incompatible linkages unless the system developer/maintainer controls the migration in a sensible manner. Management tools that monitor the product versions used throughout the system will be important accessories.

Architectural Concerns For The MII

The Coordination, Planning, and Execution System (CPES) can be envisioned as having desired characteristics that will drive the architectural design of the MII and the applications that ride on it.

Standards and Specifications: The MII should be flexible to accommodate new missions as well as enable the steady evolution of information systems technology, both hardware and software. The architectural paradigms currently being posited by the information systems community are based on the use of "object-oriented, open systems." There is an emphasis on standards that define an "open system." The commercial world is defining standards for most aspects of the information systems world. The DoD has decided to use commercial standards as the norm and to use military standards only in special, well-justified instances. The dynamic nature of the marketplace is reflected by the changing world of standards and specifications. They evolve with the technology and, therefore, add another dimension to the challenge that must be faced.

Object Request Brokers: Further, fourth- and fifth-generation software languages are utilizing the general concepts of "objects". Characteristics and standards for object-oriented implementations are being defined and implemented. A particularly interesting approach to deal with existing or "legacy" systems is the Common Object Request Broker Architecture (CORBA). Tools and specifications for CORBA are emerging from a large, industrial consortium. The approach, simply stated, provides the open system standards and specifications for which "wrappers" can be built around existing software objects. These "wrapped objects" can then be used, even modified, while living in a larger world of new and developing objects and systems. This approach needs to be exploited in evolving existing C⁴I systems into the MII.

To provide further illumination about the approach, CORBA is providing common facilities that deal with:

- User interfaces
- Information management
- System management
- Task management

These facilities use object services that provide for concurrency, persistence, transactions, queries, security, time, data interchange, and several other characteristics. If allowed to mature and be used as industry standards, CORBA provides the vehicle for building an MII that allows for the evolution of current capabilities to the system that is envisioned here.

Commercial standards/specifications cover more aspects than software. Network protocols, communication standards, and security services represent only a few of the areas that underpin the development of the MII. Implicit in all subsequent discussion is the presumption that commercial standards will provide the underpinnings for the MII. The topic will not be discussed further.

A Geospatial Reference Grid

The MII will have to support the concept that the position of everyone and everything will be available within databases accessed by the CPES at all times. While this feature requires a robust GPS-like system, coupled with the required communication mechanisms and infrastructure, it also implies the need for a "geospatial reference grid." Every individual or object needs to be tagged with a location indicator that provides for immediate and automatic synchronization and alignment of the objects of interest. Recent studies by the Defense Mapping Agency and the Defense Science Board have many useful insights as to the means for developing and implementing the architecture and the processes for realizing the geospatial reference grid. This is fundamental to the definition of the MII. Figure 19 depicts the vision for a "geospatial foundation" that has been proposed by the Defense Science Board Mapping Task Force.

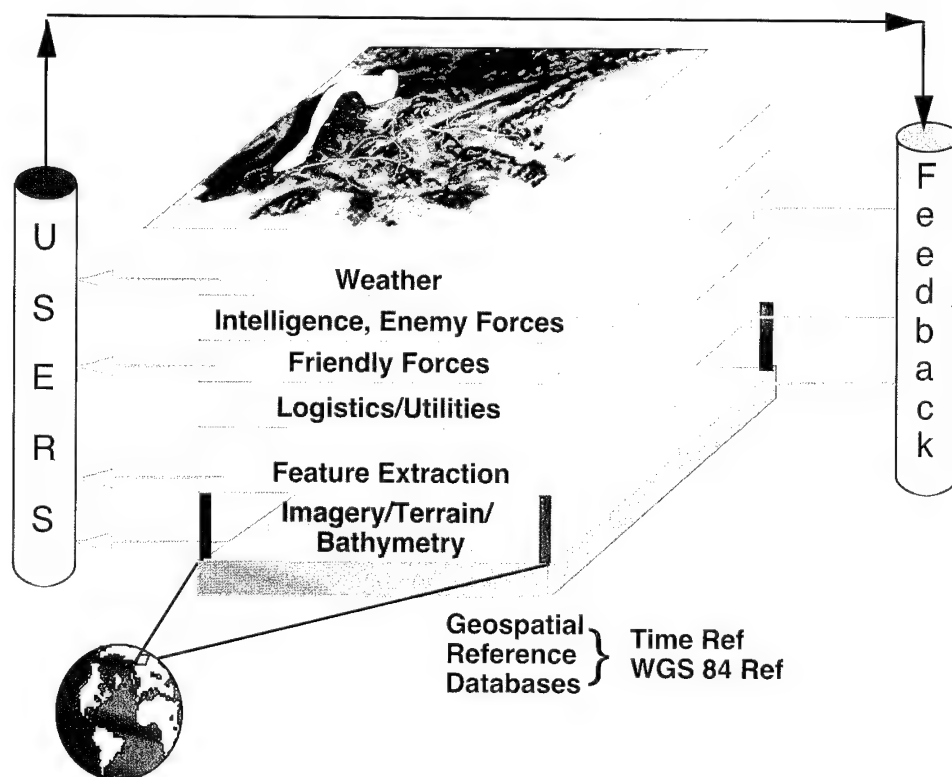


Figure 19. The Geospatial Reference Grid

Storage technology will evolve to the point where each war fighter will carry a high fidelity world model with all data in a geospatial information database management system. This system will be a segment of the world-wide database that is extracted and loaded prior to deployment to the specific geographical theater. The model master database will contain an up-to-date compendium of precise co-referenced information about earth: features, elevation, material type, density, gravity, temperature, velocity, infrastructures, structures, images, etc., plus the requisite client application tools and agents to support: measurement, monitoring, modeling, terrain

evaluation, mapping, visualization, etc. The selection and down loading will also be limited to selected data types and tools appropriate for the user mission set and application interface. During the mission, the management system will update and register all new entries automatically and issue alerts to the user agents as indicated.

The Coordination, Planning, and Execution System

With the aim of increasing the cognitive capabilities and efficiency of the decision-maker, the collaborative planning system, operating from the distributed databases that are assumed to be available, will be based on several key elements.

- Knowledge-based planning and scheduling aids, at the campaign and theater levels, which exploit techniques such as hierarchical planning, case-based reasoning, and knowledge-based simulation of friendly and enemy forces
- Embedded, on-line intelligent trainers for learning advanced system features in non-crisis periods as well as providing on-line task assistance during crises
- Collaborative tools that enable not only information sharing but virtual collaboration among users
- Multisource correlation/fusion and enemy behavior learning, recognition and prediction using statistical, pattern recognition, and knowledge-based techniques
- Highly interactive, intuitive, and intelligent human/computer interfaces that support multidimensional situation analysis and course of action visualization

The system characteristics described above are depicted in Figure 20 which illustrates the closed-loop nature of the collaborative planning function.

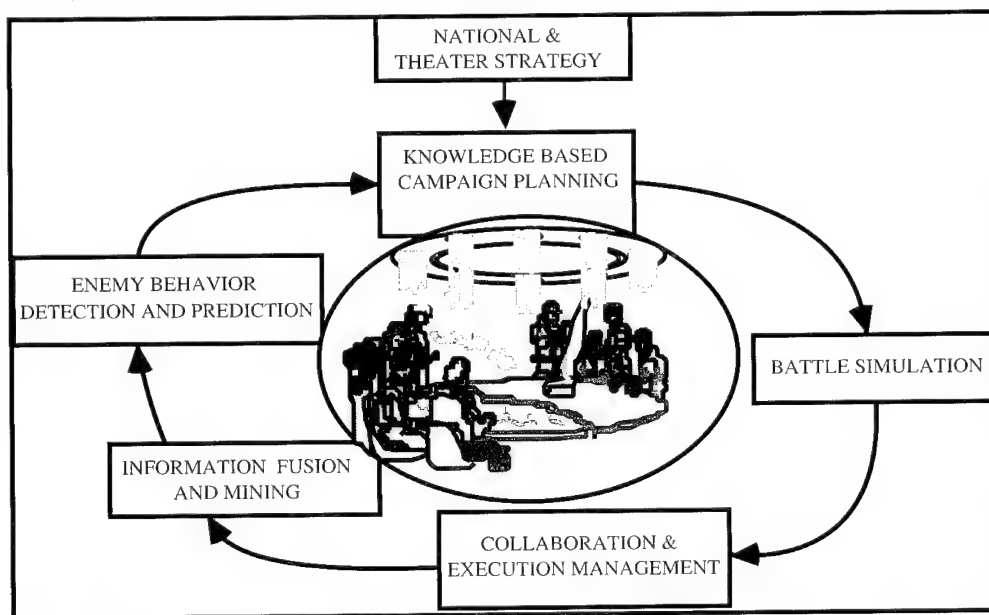


Figure 20. Intelligent, Distributed, Collaborative Planning

CPES flexibility and availability of information should be provided by the MII, the databases that it supports, and by the communications architecture and system. The CPES will have to provide the applications and tools for human/computer interactions that support the requirements for timely responses and effective decision-making. Each topic will be discussed in the following paragraphs.

Human/Computer Interactions (HCI)

The interaction devices between computers and their human users will change dramatically from the keyboard, mouse, track ball, and other tactile devices of current computer systems. They will be augmented, possibly even replaced in many instances, by other, more human-like, input-output mechanisms. There are several research threads whose maturity and capability can be recognized as having fundamental importance for realizing the system capabilities that are desired. These subject areas are highlighted during the following discussion with little supporting explanation.

Fundamental to the interactions will be *speech recognition and generation devices and natural language dialogue management*. Steady progress in these areas has been made and substantial further progress is anticipated. Because the future appears to call for even larger involvement with coalition efforts, *near-real-time language translation and generation* also will be an important feature of the system.

Other interaction capabilities will certainly appear and become available. Smart displays that *recognize and respond to gestures* are emerging. These "smart displays" will support the computer in adapting through its interface to the personal characteristics of the human operator, rather than requiring the operator to adapt to the interface. Virtual reality concepts offer the potential for the human/computer interaction to take place in an abstract domain where the computer and its human operator can associate objects through common virtual icons instead of application translations. Common icons expressed in a virtual domain will enable real-time, multinational and global participation in information collection and distribution without language translation. CPES must enable real-time international participation to support effectively coalition operations.

Today, the planning of a complex mission requires the involvement of many people who generally are brought together into a common facility and location. In the future, the MII will support *distributed, collaborative planning* in which participants, although geographically separated, can be "teleported" into a virtual conference facility (e.g., as depicted earlier in Figure 1). The *virtual displays* used for this purpose must be able to support multi-party interactions that contribute to the development of plans for action. These interactions will facilitate conversations and respond to gestures, voice, and tactile inputs. *Multi-media (i.e., voice, video, imagery, data) presentations* must be planned and distributed as part of the interaction.

An aspect that can and should be incorporated in the system is a *smart user-adaptive interface*. Supported by appropriate software agents and display technologies, the interactive system can learn from *user modeling* assessments and past behavioral tastes and patterns to facilitate the use of the system by the operator. As an intrinsic part of the interface, an *embedded on-line training* system should be built that helps the operator learn to use advanced features of

the system during quiet times. This training component serves to assist the smart interface to adapt the system to the traits of the individual user.

Support to Decision-Making

User satisfaction with the CPES will be driven by the friendliness of the HCI and the utility and timeliness of the information that is accessed using the 3-D spread sheet. However, effectiveness of the system is determined ultimately by the automated decision support that is provided by planning and rehearsal tools. Many of these tools will be enabled by the use of a class of software products that have come to be called intelligent agents.

Intelligent Agents: A central need of the CPES is the location and retrieval of information that is appropriate for the task at hand. The emerging technology of “*intelligent agents*” provides some capabilities at the present time and there are active research efforts to extend and improve the existing capabilities. Because of the importance of these methods and tools in the constructions of the CPES, a modestly expanded discussion of the topic appears warranted.

An “intelligent agent” is a robust software program that communicates with other entities to gather information and make decisions. There are several classes of intelligent agents that have been defined.

Information filter agents: Agents that provide an interface between a user and broadcast information sources (e.g., e-mail, news services) based on learned user needs and interests.

Information acquisition agents: Agents that query and access various information sources for information relevant to user-specified or anticipated information needs (e.g., automated network surfing).

Network interface agents: Agents that deliberate on how best to fulfill user information requests (e.g., complete partially specified requests).

Programming Agents: Agents that interact with a user to develop programs (e.g., programming assistant).

Cooperative scheduling agents: Agents that communicate with other agents to schedule the allocation of resources in their individual purviews (e.g., meeting scheduler).

Multitask execution agents: Agents that execute a series of tasks at different sites (e.g., electronic shopping).

Cooperative problem solving agents: Agents that work together to solve a complex problem-solving task (e.g., collaborative design).

Information fusion agents: Agents that enable the exploitation of diverse but synergistic intelligence and sensor reporting systems in order to improve situational awareness.

Cybercop agents: Agents that look for degenerate or subversive forms of agent interactions and either neutralize them or report them.

Other taxonomies are possible. We have chosen to define the agents in terms of functions that are directed toward the tasks that can be envisioned for the CPES. Agents will provide the

tools for dealing with massive data bases, with smart user interfaces, and with a variety of planning and network management activities.

Scheduling: The scheduling process certainly will involve thousands, even hundreds-of-thousands, of variables. The tools used to solve the scheduling problems must be robust and able to provide automated directions to all participating military units with near-simultaneous timing to ensure synchronized actions by all operations and support elements. *The marriage of artificial intelligence methods with the tools of operations research* is an important need for the system. There is a growing body of knowledge in this subject area and useful tools are emerging. Further progress is needed.

Coordinated Planning: Decision-makers will need to have access to situation-dependent information. It has been implied, but not stated explicitly, that *network and system management of large networks and peta-byte size databases* are required. It is in this area that the dimensionality of the system emerges as a primary concern. As noted above, a concern that significantly complicates the network and database management problem is *the security of the system*. The defense of such a system against hostile attack requires continuing and strong emphasis. Cybercop agents, for example, need to have an understanding of the proper functioning of the legitimate agents described above as well as actions that might suggest subversive activity. They can rein in errant good agents (network management) as well as police malicious agents and suspicious activity. An example of suspicious activity might be over dependence of a decision-making agent on a single source of input. This could suggest spoofing by an enemy agent.

Given that decision-makers have the information they need, the planning function will be distributed to appropriate elements of the organization. Distributed planning will be facilitated through the use of *work flow management and intelligent routing* tools.

Data and information about a specific object or activity can be obtained from several, very disparate sources. The information retrieval system should assist decision-makers in integrating information about each object/activity through a generalized *correlation/fusion* process. Information types vary from sensor measurements to intelligence sources to orders of battle to geographic and terrain data. These disparate types of information need to be merged in an intelligent manner that depicts to the user an answer with the attendant uncertainties and caveats. Using temporal and geospatial reasoning, information fusion agents will aggregate multiple sensor events related to the same object over time to produce object movement histories. They will then select the most battle critical entities, perhaps using case-based reasoning, and predict higher level enemy behaviors and intent. The use of the geospatial reference grid is expected to facilitate the correlation/fusion function.

The system must have the capability to “roam” and “zoom” to support the decision-makers understanding of the situation. It seems reasonable to assume that high-level decision makers (e.g., the JTF commander) will want to have information that allows him to define strategies and tactics that respond to the general situation. Wing commanders will need different and more specific views of the battlespace. To illustrate the general point which can apply to all types of information, consider the roaming and zooming capabilities offered by different types of sensors. Space-based platforms provide swaths of information at a particular resolution. The information is obtained during intervals that are discrete and may be separated by tens or hundreds of minutes.

A unmanned air vehicle (UAV) can survey an area continuously and with greater resolution in selected areas. The UAV can roam or fix upon specific areas. The two sensor systems provide overlapping and complementary capabilities that have utility that depends on the role of the decision maker. The preceding discussion raises the important topic of *collection management*. The manner in which sensors are tasked to achieve improved situational awareness for a specific situation becomes an important feedback loop within the CPES system.

The planning process often identifies more than one course of action. Decision-makers can be supported in making the ultimate choice of a plan through the use of *faster than real-time simulation tools* that permit the meaningful assessment and comparison of alternative courses of action. The output of the simulations using two-dimensional (e.g., *HDTV*) or three-dimensional (e.g., *virtual reality*) displays will provide a much sharpened intuition and understanding of the situation that is being faced. The development of appropriately fast and accurate simulation tools, including the intelligent display of the results, is an objective which is becoming more and more realizable.

General Conclusions

The implementation of the Military Information Infrastructure (MII) and the Coordination, Planning, and Execution System (CPES) can be supported by the information system applications and technologies that are emerging at the present time. There seem to be no major inventions required to realize the MII and CPES. The greatest limitation may be our imagination or perhaps a reluctance to leave the paradigms and cultures of the present for a very different future reality.

There should be no confusion about the difficulty of the task. A great deal of effort will be required to achieve the desired vision. The approach is based on an assessment of current capabilities and a projection of the possibilities for the future. Even if the exponential growth in processing power is not realized and the ideal system outlined here is unachievable, the capability that is fielded should be “good enough”, particularly when compared with the “stove-piped” systems of the present time.

Success in this endeavor will produce a military organization that can operate effectively with the reduced force and command structure that is predicted. It will be able to respond to a broad range of missions, from regional conflicts to humanitarian support. The ability to respond rapidly, deploy quickly, conduct surgical operations, etc., will be enabled.

The MII/CPES can provide the means to achieve global situational awareness and to take actions in the timely manner required to be effective. Obviously, sensors that provide the “eyes” for the system are required as are the platforms and weapons that provide the arms, legs, and muscle for accomplishing the desired actions. However, the coordination, planning, and execution system that has been outlined here can provide the US with an insurmountable advantage in any situation. Since the technologies are available through the commercial market place, the investment by DoD must be concentrated on the application of the technology to military missions. More than anything else, this is a requirement to integrate information system components into a system of systems that will support the goals, objectives, and missions of the armed forces.

Basic Recommendation

The development of the MII and CPES will be challenging. The history of information systems technology provides some lessons that may guide us in planning for the MII and CPES. One highly successful distributed information system is the Internet. It is now being used for purposes that its original developers never envisioned. It has undergone revisions to its naming system over the years, is growing steadily, and is now hosting a series of new hypermedia applications (e.g., Mosaic, Netscape, and the World Wide Web), giving access to millions of new users. This suggests that a bottom-up, evolutionary approach to large systems may work well, as opposed to a top-down approach working from a formal specification of the objective system.

We do *not* believe that the development of the system can be achieved using an entirely “top-down” approach. As is said in many situations, “the devil is in the details.” We must learn from past experience and capitalize on new trends in the information systems marketplace. Thus, we recommend the following approach.

The Development Approach: The Air Force must make a *long-term* commitment to the vision of the MII and the CPES. This necessitates a continuing commitment of resources for an extended period of time, analogous to the development and acquisition of major weapon systems like the F-22. The emphasis on “long-term” is deliberate. The commitment must reflect the following attitude, “If the system stinks; fix it.” It cannot be allowed to reflect the attitude, “If the system stinks; kill it.”

There are two aspects to the commitment:

(a) There needs to be a top-level architectural effort that clearly describes the overall “vision” or objective system. It must delineate the desired capabilities of the system, define the architectural approach (e.g., standards, tools), and institutionalize the process through which the developing system is confirmed to satisfy the architectural requirements. This cannot be done just once because important lessons will be learned along the way. New technologies and standards will probably emerge and could require changes to the architecture. Therefore, reference models, standards, guidelines and well-defined processes are needed to manage the overall evolutionary development.

(b) The MII and CPES should be procured in a series of small increments, each more elaborate than the previous one. Each increment should be developed in a relatively short time and should satisfy the current formulation of standards, guidelines, and procurement strategies for future increments. For any and all of these increments, risk mitigation strategies (such as competitive design phases) can be employed. Should an increment run into significant development trouble, it should be possible to “cut one’s losses”, cancel that increment and redirect the overall MII/CPES program. The developers of each increment should be incentivized toward contributing to the success of the total MII/CPES system, not only to the success of any individual increment. In this way the MII and the CPES can evolve toward the ultimate objective system.

The system architects, engineers, and technologists who develop and maintain the documents defining the objective system and its processes will serve as the knowledge keeper that guides the architectural evolution and assures the fidelity to the vision of developing system

Operator-Engineer Interactions: A distributed prototype of the MII/CPES must be built that involves users from across the Air Force directly with the engineers charged with constructing the system. This has several advantages. Obviously, the use of a development increment by end users may reveal flaws, or areas for improvements. Second, it is advantageous that end users have visibility into the kinds of information technologies they will employ routinely in the future. We believe that just as the MII and the CPES will evolve over time, so must military war fighting doctrines and military organizations evolve to take full advantage of the MII and CPES. Exposing Air Force users as early as possible will foster discussion of the issues that emerge. Finally, actual field use is the best way to judge progress. The prototype should be used in war gaming and exercises to the extent possible in a way that permits comparisons between the new version and earlier, fielded capabilities.

The prototype must be planned to evolve within the architectural guidelines to achieve the general vision for the system. By building the system from an “embryo” and guiding its maturation, the difficult problems that require concentrated efforts for their solution can be unearthed and investigated in the “real” world rather than in the “abstract.” A consequence of the activity may be a structured, even an automated, process for identifying mission deficiencies and defining requirements.

The visionary system is too complex to anticipate where the stickiest problems will emerge. By expecting the unanticipated, failure is certain on the short-term (i.e., “the system stinks”). By committing to the long-term goal, the solution of important problems will occur within the context of the operational system (i.e., “fix it”).

There is an attendant advantage to the proposed approach. The system must from the outset link as many organizational elements as possible. An important goal of the prototype development would appear to be that every unit of the Air Force should be connected to the system as soon as possible. Certainly, it should be used in conjunction with exercises to gain some realistic assessments of its performance and deficiencies. It is even easy to imagine that this system can be used for some contingencies at a relatively early time during its development.

By linking operational units, the ultimate users of the system become intimately involved from the start. Their emphasis must focus on getting their operational job done. The engineers who build the system must deal with the most satisfactory ways to implement the real needs of the users. A constructive dialogue must be established and maintained throughout the life of the development.

Air Force Link to the Commercial Marketplace: The Air Force must be more than a passive consumer of evolving COTS and other information systems technology. As stated earlier, the Air Force has many needs in common with other consumers of real-time, distributed information systems. The Air Force should attempt to influence the direction of future information systems technology, leveraging its influence by working closely with other consumers to keep vendors aware of Air Force needs and priorities. The experience gained by Air Force engineers from the development of the MII/CPES should make them a knowledgeable and influential member of the information systems community. There must be a strong effort to establish this link between the Air Force and this community.

Epilogue

The implementation of the Coordination, Planning, and Execution System (CPES) has significant implications for the Air Force of 2025. The access to large amounts of information at even the lowest level of the organization empowers units and individuals to achieve near real-time responses that some situations may require. A more horizontal organizational structure seems natural with a greater emphasis on the leadership role of the commanders. For example, the Air Tasking Order may provide the top level strategy that is executed by the rest of the organization but not include the immense amount of detail included at the present time.

To repeat the sports analogy used earlier, the change will be like shifting from football to soccer. There will be no pauses in the action to huddle and to define the next play, so that everyone has a common view of the anticipated action. Instead, actions are continuous within the strategies set before the start of play. In addition, there will be superb real-time communication at all times between the command staff (the coaching staff), the shooters and sensors (the players), and the supporters (the trainers and equipment managers). They will share a common view of the battle space including covert means of communicating intentions between the shooters, an advantage not available on the soccer field! Assuming the opponent does not have an equivalent awareness, dominance in the game should follow.

To close, the fact that most of the information system technologies and products are being provided by commercial industry implies the DoD does not have to bear large development costs, but primarily the costs of integration and application. This implies that the creation of the MII and CPES, while manpower-intensive, will involve the educated purchase, but not the development, of information systems. As already stated, a long-term commitment to the effort is mandatory but the costs should be considerably less than generally experienced in the acquisition of large systems. In the end the Air Force will have a system that is more than a force multiplier. It will be the enabler for the capability to respond quickly, effectively, and decisively to situations ranging from regional conflict to operations other than war.

5.0 Offensive Information Warfare in the 21st Century²⁰

Lt Gen Lincoln D. Faurer, USAF (Ret.)

There is no disagreement that information infrastructures are emerging as centers of gravity for (trans-) national power, and that as they grow in strategic importance a new, and thought by many, revolutionary aspect of warfare—information warfare—is taking shape. It is in the “taking shape” that disagreements arise.

Information Warfare (IW) - A Significant New Consideration

Within services and between services there are advocates for several interpretations of Information Warfare. Questions which need resolution, and hopefully common approaches across the services, are such as: Is IW something new or just an aspect of warfare that has been with us since the Trojan Horse? What is the demarcation between IW and C²W? Is it the latter only that is the domain of DoD? Since conduct of IW embraces more than the “warfighter”, where in our government is the responsibility for incorporating IW into the waging of war? Should IW stand alone and have its own advocate for competing within services for budget allocations and attention? Is it information or cyberspace that is a realm like air, land, sea and space? Should the argument between those who would isolate IW as a specific mission and those who would integrate it into doctrine be finessed by definitional fractionation to include Information Operations, Technical Operations, C² Attack, Offensive Counterinformation, etc. all being subsets of Offensive Information Warfare?

Such questions frame the challenge of incorporating IW meaningfully into our national security posture and validating it against more conventional weapons in our force structure. Our exploration of IW will be predicated on the belief that “the information dimension of modern war can be utilized knowingly and proactively in support of national policies, goals, and interests.” This follows logically from the fact that technology advancements have created an information abundant world environment increasingly reliant on timely, accurate flow of information for the conduct of business, the functioning of government, the operation of the national economy, and the conduct of war. This situation has introduced a new and substantial vulnerability into national conflicts. It is a vulnerability that cuts two ways and requires protective actions in parallel with preparations for offensive actions. This paper concentrates its analysis on the Air Force role if development and readiness for national employment of IW offensive capabilities is to be assured. In the course of this analysis the many questions surrounding IW will receive attention.

Cyberspace, “that consensually imagined universe where information reigns supreme,” presents the world with a unique set of problems. National borders cannot be projected into it and ownership of virtual reality is infeasible. Its properties are quite different from those of land, sea, air and space, but it most certainly is a realm in which national security must be contested.

When confronted with potential conflict, a national strategy employing offensive IW would be very advantageous. It would permit us to shape the *battle space* of conflict rather than react to a *battlefield* of the enemy’s choosing. It would provide options which minimize the fatalities

20. See also accompanying classified monograph on “Technical Information Operations.”

of traditional combat. Likely, the long term cost of its preparation would be less than that of hard kill weapons. Finally, its use would effectively complement a declining force structure and offer alternatives to overly stretching forces when confronted with multiple crises.

Offensive IW - What is it all about?

The objective of offensive warfare has always been to deny, destroy, disrupt or deceive the enemy either in his employment of forces or in retaining support of his constituency. The advent of the Information Age simply introduces a major new target consideration. The opportunities it brings us to improve upon our more traditional weapon systems and their management in the conduct of war brings commensurate vulnerabilities. Winning the battle of information dominance requires that we achieve an edge in offensive exploitation of the enemy's vulnerabilities over his ability against our protective measures. Given the global application of commercial progress in the information realm, and the extent to which modernization/upgrading will be pertinent to all countries, one man's "protect" need will be another man's offensive "target". Furthermore, even setting aside the specific, technical actions discussed in the IW Protect portion of this study, an important element of protection is to be able to "attack the attacker" so as to deter or to respond in kind. Couple all of this with a realization that the U.S. is probably the most dependent of nations on both its own and the global information infrastructure, the U.S. must accomplish a deliberate integration and balance of its Protect and Offensive knowledge and investment. Our historic predilection to emphasize the latter must be tempered by the severity of risk in doing so in an Information context, as well as the illogic of not recognizing the inextricable meshing of technology applications to protect and attack.

Although the objective of Offensive IW remains the classical "to deny, destroy, disrupt, or deceive", its most different feature is the extent to which the effect of an act will ripple beyond the immediate target. We learned with the advent of nuclear weapons the critical importance of considering collateral damage. We have extended that learning to all weapons of mass destruction as we factor into our decision process such matters as effects on: enemy civilians, our forces, coalition forces and public attitude. Offensive IW, operating in the virtual reality of cyberspace, exacerbates the above considerations. Operations, often civilian in nature, far from the battlefield are caught up in the affected battlespace. Often this worry is in conjunction with an opportunity for leverage of the greatest value, e.g., termination of conflict before war breaks out into killing, or nearly non-lethal attack options after the onset of hostilities. If the U.S. is to fully prepare an Offensive IW capability, a number of actions must occur.

The opportunities and the challenges of Offensive IW and the investment needed to convert a "possibility" into a national policy and strategy must be understood and accepted at several key decision nodes of our government. These must include the NCA, SecDef, CJCS, Service Chiefs and CINCs in the direct force structure chain, and such other national security principals as the National Security Advisor, and Secretary State. The maturing of an Offensive IW national strategy will also require expansion of involvement to embrace such as Treasury, Commerce, Economic Advisor and several other government and private sector specialist functions hinged by vulnerability and expertise to the global information infrastructure. After understanding and acceptance have been achieved there must be commitment to investment.

Investment in information technology analysis and adaptation must parallel the development of operational concepts. Projects must be as carefully tailored as they are for weapon systems. Information warriors, specially trained and with new attitudes, must be molded from people drawn from the fields of Intelligence, Communications and Operations. Exercising and simulation during concept refinement should feature the problems of complex, Joint integrated planning, execution and over-sight. A linchpin to successful Offensive IW will be preparation, sustainment and easy utilization of a detailed, responsive, massive, integrated data base. Commercial technologies permit implementation of such a data base arrangement, but legacy systems (hardware and software) and resource limitations stand athwart an essential database revamping.

A National Strategy of Offensive IW Needs Leadership and Focus

Information Warfare is receiving attention throughout DoD—in OSD (DISA, ARPA, ASD/C3I), the JCS, and the Services. The efforts appear specialized and non-complementary. There appears to be an absence of over-arching focus that is necessary for creation of a national policy and its implementing wherewithal comparable to the post World War II complementary policies of Containment and Nuclear Deterrence. Yet the potential of Information Warfare is as dramatic and basic to our national security posture as were those policies of 50 years ago.

After World War II, with respect to airpower, we recognized the need for dedicated attention to necessary R&D investment and to development of operational concepts. We stood up an Air Force and gave it focused responsibility to concentrate on air power, even though air arms continued in the other services. The need for similar concentrated focus in cyberspace is every bit as great today, and the breadth of the challenge is every bit as broad. “The playing field of IW is the full dimension of information itself, and embraces any element which supports, feeds, or interacts with the dimension of information. The playing field is practically infinite, delimited for each operation by the weapons chosen, the methods of engagement utilized, the strategy and metric for success.” The players extend well beyond the so called fighting forces of DoD and mirror the targets of IW, which include physical entities, data, decision processes of national leaders and the popular will of the citizenship. As the nation goes about the task of “right-sizing” our national security posture and weighing its costs against other needs, investment in new and not thoroughly understood “info weapons” will come under great scrutiny. It is time once again to take an action that will assure undivided focused attention to a new and critical realm of conflict.

The focused responsibility for “info power” should not be misconstrued as arguing for a mission grab by one service. Ultimately, the conduct of IW will be pertinent to all services and will need be employed tactically and strategically within each service doctrine. Such employment, however, will need be prefaced and supported by development of a common understanding of objectives, buttressed by adequate research and development of implementing technologies. Since IW has a dimension that impacts well beyond the traditional bounds of DoD and embraces decisions throughout our government, focused responsibility is necessary to ensure preparation of a nationally acceptable program. It is logical that the focused responsibility be resident within that department, the DoD, that has as its mission the conduct of war for the nation, even though employment of this new IW “weapon” will involve the remainder of government and could impact the private sector. Whether the target is within the private sector or not, the result, if not

the objective, is inimical to our national security. In fact, the range of harmful results may be the equal of any war we have fought. Therefore, while there are roles for many elements of our government and portions of the private sector, the logical residence for leadership regards to national security is the DoD. Finally, if it should seem practical to choose amongst the existing services for assignment of focused responsibility, rather than some other organizational solution, the Air Force is arguably the most suitable.

It is not intended that "focused responsibility" be interpreted as usurpation of assigned roles and missions elsewhere in our government structure. It is not intended to generate conflict between "law enforcement" and "military". What is intended is responsibility for "end to end" consideration and subsequent guidance relative to ensuring information dominance (protection and exploitation) with respect to any hostile (trans) national entity—country, group, or person. One might liken the task facing us in the information realm to that confronting us after World War I and the inheritance of an "interesting capability"—the airplane. Even as the military was groping its way to a proper role, the private sector was expanding its applications. The envelope of capability needed to be pushed and a supporting structure of aids, regulations and controls needed to be developed. It fell to the Army Air Corps to lead the way. The "focused responsibility" for cyberspace, or the information realm, or information warfare should be viewed in much the same context as our experiences with airplanes and air power after WWI and WWII respectively. It is meant to be leadership not sole authority.

The Air Force, whether or not designated the lead service for IW, should embrace with enthusiasm and invest significantly and immediately in preparing capability. The Air Force's Global Reach—Global Power (Global Presence) mission logically embraces the standoff offensive potential of Information Warfare. The exploitation of information infrastructure vulnerabilities is a natural extension of Air Force strategic targeting, an area in which visionary debate to clarify roles within our government structure regarding the conduct of IW in a time continuum of peace into declared war, and of C²W vs. IW within DoD, is of great importance.

Although tactical applications are obvious, it is in the strategic dimension that offensive IW most likely will have its greatest impact. It has the potential for application prior to the "shooting" phase of conflict. Early application should permit shaping of the "battlefield" (more properly, battlespace) to our advantage such that engagement of forces may be avoidable, or in the event of engagement, bloodshed can be minimized. The dominant strategic considerations make U.S. mastery of offensive IW critical to the Air Force. Such mastery requires priority investment of people and money and an intellectual commitment to the development and acquisition of technical understanding and capabilities. If we fail to do so, we'll be caught short in an increasingly dangerous realm whose risks and opportunities we have contemplated but not yet adequately studied. Furthermore, we will be missing the opportunity to properly judge reduced investment and reinvestment in "killing" weapon systems as tradeoff to offensive IW investment.

We offer a final consideration in the assignment of a "leadership" role for either the protection of our national interests regards an information infrastructure or the development of an offensive IW capability. To separate the two would be a mistake. The synergy between the efforts are too pervasive to ignore. They are more than two sides of the same coin—each is, on occasion, the other in technology and process. Whatever organizational decision is made in designating focused responsibility and leadership for IW, it should embrace both aspects of

Information Warfare, much as NSA has both SIGINT and Information Security, so that cross fertilization of technical talent and operational experience can be achieved.

Summary

With information infrastructures emerging as centers of gravity for (trans) national power, the U.S. is faced with critical risk and critical opportunity. We can confront them as one by establishing as a national objective the achievement of information dominance. Pursuit of that objective demands that some hard decisions be made soon. Soon, because the U.S. is probably the most dependent of nations upon Information and Information Infrastructure—currently the cost of access to our information systems is extraordinarily low. Soon, because of the rate at which computer and communications technologies are compounding the volume and complexity of the global structures we must protect and attack.

The overarching decision that must be made is how best to bring cohesion to the many disparate Information Warfare efforts underway in DoD, elsewhere in our government, and even to some extent in the private sector. The following two observations are offered:

- A national objective of the significance and potential impact of information dominance requires top down establishment of a national strategy and governing policies. In effect, it must have focused leadership—an assigned responsibility for end-to-end consideration of all the needed and integrated components of a most complex national scheme.
- Although protect and attack actions will involve and impact the private sector, a national security rather than private/commercial sector perspective must dominate strategy and policy formulation.

Logically, it follows from these observations that the SecDef and DoD be Executive Branch designee for paramount responsibility within the government for IW. Whether this responsibility is delegated within DoD to one of the existing services (arguably the Air Force would be a good choice) or organized in some different fashion (perhaps a joint service NORAD), a prompt decision is needed. We must have such if we are to have timely planning, cohesive investment, and a reasonable chance of meeting the objective.

A third observation is that the contributions of protect and attack actions to the objective of information dominance are mutually supporting and technically commingled. Thus it can be argued that the protect and attack dimensions of IW should be addressed as two integrated features of a single strategy. Aside from technical cross fertilization, operational performance of each will strengthen the other. Together they constitute the challenge of ensuring information dominance.

In planning an IW strategy, whether as an Air Force or a national plan, it should be recognized that target information systems will change fundamentally in the near future, and that the following actions should be featured:

- Robust attack technologies capable of on-demand use against a range of target technologies/systems

-
- Leveraging of intelligence community parallel technologies to access and process targets
 - Pursue long term expert based study on improved techniques for computer attack which increase on-demand effectiveness with reduced manpower investment
 - Pursuit of intelligent agents for attack mission

6.0 Information in Warfare: Toward Dynamic Command and Control

MG John Stewart, USA (Ret.) and MG John Corder, USAF (Ret.)

Desert Storm provided a window onto 21st century aerospace warfare. Authors have described the contribution of precision weapons in the Gulf War. Indeed, smart munitions became the symbol of how Desert Storm differed from previous conflicts. However, though precision characterized much of JFACC operations in the Gulf, it is information, its demand, use, and shape, that characterizes Desert Storm as the precursor conflict of the 21st century.

In Desert Storm, the JFACC conducted simultaneous, asynchronous planning for operations over wide areas for over 40 days in which hundreds of strike and support aircraft conducted multiple and disparate missions. Commanders required focused sensors, near-real time situational awareness, flexible and agile air tasking, and quick, accurate battle damage assessment. Combinations of targets, both strategic C⁴ centers in Iraq and tactically deployed ground combat units in the Kuwaiti Theater of Operations, required persistent sensor and fusion efforts. In turn, these targets proved to be highly dynamic, frequently changing in priority and in the case of tactical targets, in composition and disposition as well. Desert Storm provided our first real example of selective, precision attack, which in turn drove the high demand for information to accurately locate and describe the overall situation and specific targets.

Not just attack, but control also put demand on information. Fixed and Rotary wing aircraft, unmanned aerial vehicles, and ground air defense systems all from different US services and coalition partners required detailed planning, structured but flexible control measures, and quick dissemination of a common, relevant situation. Thus, Desert Storm punctuated for commanders the crucial nature of a highly accurate, responsive, agile, and fast information system. Of course, the Desert Storm information system did not function as commanders required. It was not designed to do so and was pieced together, practically at the penultimate hour, to perform as it did. What we lacked in cyberspace, we made up in aerospace, in leadership, dedication, training, and also to a significant degree in massive force. In a 21st century conflict, we may not have the benefits of overwhelming aerospace overmatch and mass as well.

USAF Enduring Roles

While uncertainty, itself, will be the defining characteristic of future military missions, the US Air Force will retain key enduring roles.

- Continue to maintain readiness and dominance to conduct aerospace warfare in all its manifestations of strategic and operational attack, offensive counterair, air interdiction, and reconnaissance and air support to land-force operations.
- Retain and enhance its force projections capability to selectively and precisely attack, to demonstrate US power, and to deploy with dispatch and decision US force anywhere in the world.

-
- Provide world-wide sustainment operations. Quick operational tempo, flexibility of organization, and mission agility require continuous, paced, and tailored sustainment operations forward to aerospace and ground battlespace warfighters.
 - Provide trained and ready Special Operations Forces role will also become increasingly more important.

These enduring roles, which in sum describe a global and spatial reach capability, place an increasing premium on timely, accurate, graphically and flexibly displayed information in warfare. But since information has always been important in military operations, what has changed that has made information a critical element of combat power? The real change can be stated tersely: information's effect on decision and on operation precision. Now and much more so in the future, commanders will reach out to sensors and interactive databases to tailor accurate, real time situational awareness for themselves. Cybersystems will quicken, quantumly, command capabilities to decide and to execute decisions. These systems will represent a powerful suite of military capability to be used as a weapon and to be protected as much as the current key weapons systems are now. Information is changing the very nature of military operations as much or even more than historically critical advances in warfare (e.g., the bow and arrow, firearms, and aircraft).

Information Requirements

One key conclusion from the Gulf War was that the priority for information is now on field forces. During the Cold War, military information flowed upwardly and centralized at the National Command Authority, due to the key mission of strategic nuclear deterrence. Now, deterrence remains an element of US national security strategy; however, power projection is the key strategic element. In this new environment commanders at the theater commander and Chief (CINC) or his designated Joint Task Force level and below make and execute strategy. Young naval commanders and lieutenant colonels operate today in the strategic through tactical-levels from Macedonia to Kuwait, and the information system must focus on their needs. Traditionally, information moves sequentially and hierarchically in our military. That contributes to order. It serves the senior levels well, but it is inadequate for today's and tomorrow's military operational environment. This change—the increasing priority for information at the JTF and below—and the emerging communication and computer technologies to support it signify a crucial element of the revolution in military affairs that is underway.

Information in Warfare is a defining aspect about what is new in military operations in this new information age in which we enter. Information in Warfare is the means by which warfighters drive and derive, use and apply, and shape and share information in the course of their operations, whether in war, operations other than war, in crisis planning, or in day-to-day peacetime activities. While “warfighter” can be defined as any military leader from a CINC to a pilot, for the purposes of this paper, we focus on the Joint Task Force commander and his subordinate commanders.

JTF and below commanders require timely and relevant information which provides decisive advantage in controlling their battle space. Their information has to be common (relative to other commanders up and down the hierarchy), but adaptive to suit each particular level.

Commanders have to protect their own information and systems without restricting operations, while disrupting and denying their adversary's information.

By the second decade of the 21st century, commanders will have an automated fusion capability that provides the means to have insight into an environment of simultaneous, asynchronous, parallel operations. This will reduce (but not eliminate) friction in operations through clear situational awareness. Staring sensors and dynamic perspectives of the area of operation will provide the means to focus on massing effects and on determining environmental effects. Clear understanding of terrain, space, weather, weapons, forces, cultures electromagnetics, and other factors will come in forms of visual portrayal of these effects on operational space. Commanders will pull, tailor, and synchronize information from national through tactical data bases. They will use simulations which are integrated and interactive to seek insight into potential futures, and to rehearse, decide, and act. They will have wide access to data bases, the contents of which will be tailored to their information needs.

Information will move simultaneously around and through military organizations which while retaining some essential elements of hierarchy (for coordination, and centrality of command) will be more horizontal and matrixed for eclectic operations. The information age will effect staffs directly by reorganizing them on knowledge based plans, decision, and action rather than along traditional, functional lines. In fact, command authority itself will depend on information in the 2020's. The commander with the clearest insight will dominate.

These profound changes in military operations brought about by information age systems and technology portend major impact on doctrine, organization, and training. The 21st century warrior will truly have to be a Cyberwarrior. Commanders will need to know the information system as well as they know aircraft and weapons systems today. They will train not just on the use of their cybersystems but also on the ways to employ them as operational multipliers.

Doctrinal Implications

Doctrine will evolve, being pushed by technology and in turn driving technology, itself. The current command and control paradigm of a theater CINC or his designated JTF controlling of military operations will endure, but Information in Warfare 21st century characteristics will influence (perhaps drive) doctrinal and organizational models for joint operations. By the 21st century, joint doctrine will center on JTF operations and will lead and integrate directly with service doctrine. Joint doctrine will drive standardized tactics, techniques, and procedures for JTFs operating across different theaters. This is a crucial step in the evolution of Information in Warfare as a combat multiplier, because it will place all operating elements on a common standard. If joint commanders demand the capability for "information dominance" and a common, relevant picture of their battlespace, then the Information in Warfare tools they have must also be common. For example, there currently exists joint military terminology which defines command and other relationships, but which leaves specific service terms under the purview of the services. As the doctrinal lead settles at the JTF-level, service unique terminology and operational concepts (especially where land, air, and sea operations overlap at the seams) will meld at the joint level. In turn this will foster more integrated JTF planning and operations and will drive the development of common information system suites and commonly constructed, distributed data bases. Certainly Doctrine will retain its role as a guidepost (vice directive) for commanders. They will continue to tailor their planning and execution based on mission using

doctrine as a standard. However, joint-led doctrine will be a necessary foundation for the effective use of Information in Warfare technological capabilities.

Dynamic Command and Control

The objective of Information in Warfare technologies is to provide commanders the means to command and control forces in dynamic situations and be successful. A top-level vision of how Joint Task Force Commanders will use information in the future follows:

- Commanders must have a dynamic, near- real time, accurate situational picture of their battle space (air, land maritime & space). This “picture” serves two main purposes: clear situational awareness for support to planning and operational decisionmaking, and target planning and execution. By dynamic we mean automated, visual portrayal of terrain, weather, sensors, and forces in perspectives tailored by the commander to provide situation awareness. Real time means fast enough to be of significant military value. For example, against tactical ballistic missiles, the time frame might be seconds. Against other high value, less mobile targets, the time frame might be minutes to a few hours. Accurate means good enough to be of significant military value.
- The commander must focus the effort. in planning and in operations. From clear situational awareness and based on his campaign plan, he decides on high priority targets and focuses sensors and surveillance on detecting, identifying, and locating them.
- Commanders attack with minimal losses using the most efficient land, air, maritime or space weapons. They determine the results of these attacks quickly, and directs that the near real time, accurate picture be promptly updated to permit the dynamic operations to continue.
- The time dimension of the above process must be minutes and seconds vice hours.

This vision of dynamic command and control holds major doctrinal (and organizational) implications. It implies a melding of planning and execution functions and interactive ways of prioritizing effort during simultaneous, asynchronous operations. Aerospace operations provide an example of this issue.

The ability of US military air power to conduct deep and sustained Offensive Counter Air (OCA) and Air Interdiction (AI) set it apart today from all other air forces, and that depends largely on the ability to plan and execute the Air Tasking Order (ATO). In the overall scheme of air power employment, ATO planning, preparation and distribution represents 35% of the C⁴I problem, while execution represents 65%. Most of the effort to improve the ATO, ironically, has gone towards planning. While this will improve air operations, the major enhancement can be made in execution.

Planners construct the ATO based on the joint forces commander’s campaign plan. They use the latest targeting data, usually about 12 hours old, and operational input. Their mission is to focus air power on the commander’s intent. Once disseminated, the ATO becomes the purview of current operations for execution. Since ATO planning and execution occur simultaneously and asynchronously, planners continually hand off to operations. This allows the former

to focus on campaign priorities and the latter on implementing the plan. The issue is that military operations always change, because the situation is dynamic. Since target data from the recently transmitted ATO is old, the current operations element in the Air Operations Center (AOC) executes the ATO almost entirely differently than its actual plan and this requires clear situational awareness to execute and focus air power on the right targets.

How does the current operations function in the AOC make change and adjust OCA and AI missions once sorties are airborne? The Gulf War clearly outlined this need in, for example, JFACC responses to fleeting targets like mobile armored units or tactical ballistic missiles or attacks on dug-in ground forces, the locations of which were deep in the battle area and of which were generally, not precisely known. The answer to the current operations enigma lies in assessing doctrine and organization and how information (read intelligence) on targets moves into the current operations element of the AOC.

The JTF J-2, as the senior joint intelligence officer, manages sensor collection and the production of intelligence based on the commander's intelligence requirements. A significant part (but nowhere near all) of those requirements is to develop precise location, composition, and disposition of priority targets. The J-2 has additional missions, as well, to warn, develop the enemy situation, and provide battle damage assessment, to name a few other significant users of sensors, time, and dissemination resources. During the planning function of the ATO, AOC planners (representing the JFACC) pass requirements to the J-2 for targets. In turn, the J-2 focuses sensor collection and analytical resources. Sensors provide input which intelligence analysts turn into their best estimate of target data and disseminate to AOC planners. This organization for information functions reasonably well for planning purposes, in peacetime or in military operational situations. (Figure 21 provides a description of the intelligence flow.)

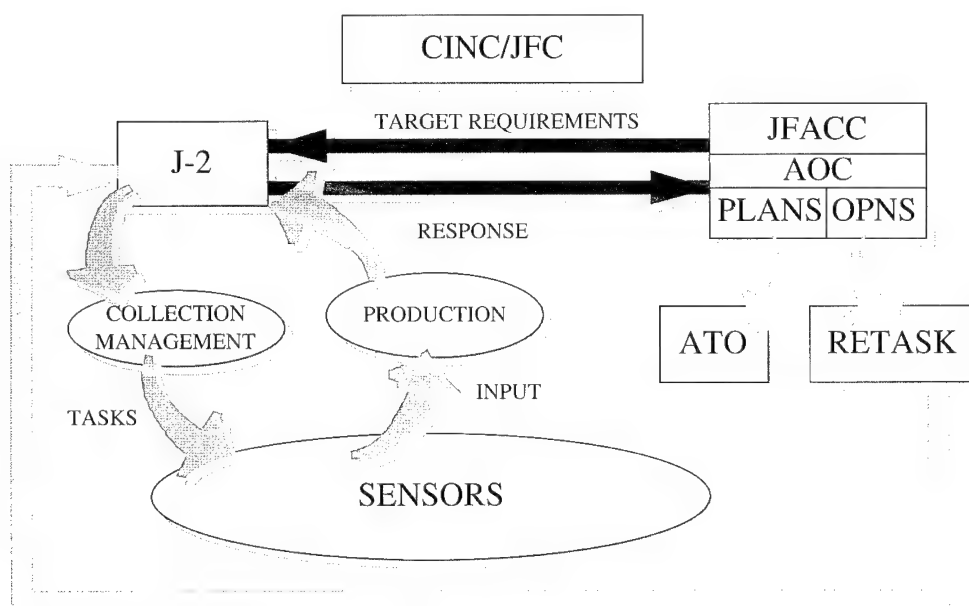


Figure 21. Intelligence flow

However, the system does not serve the execution function of the AOC as well due to lags in the flow of timely target data in a dynamic command and control environment.

The informational architecture was established in the form described to ensure effective use of limited sensor resources and their focus on priority targets and other requirements. In an Information in Warfare age where capabilities for near-real-time accurate situational awareness exists, new organizational paradigms can evolve to address the crucial problem of dynamic ATO execution.

Commanders require an intelligence support architecture to conduct dynamic command and control. In that domain the J-2 continues in the role as the senior intelligence operational staff for the joint force commander as well as provides support to the JFACC/AOC planning function. Thus, the intelligence requirements and response flows remain the same as under the traditional model (Figure 22). What does change is the organization of the current operations element of the AOC and its relationship with the J-2 and its role in sensor collection management. Current operations has direct input from and tasking authority over sensors under this schema. This architecture requires near real time, dynamic, and accurate situational awareness of the entire JFACC battlespace resident in the operations function. That is the key to ensure that operations, in executing the ATO with the advantage of direct, real-time sensor input, is concomitantly focusing on the right, high priority targets, and not just on the next target in view. Additionally, this architecture, with its tight links to the J-2 and direct input to AOC operations, provides the means (automated or human) to coordinate sensor priorities, which are almost always mutually exclusive in an interplay between targeting, BDA, warning, and other critical requirements. Of course, the future might well provide quantum improvement in both the quantity and quality of collection resources, but since friction is a constant in operations, the coordination of priority for assets will likely remain a challenge.

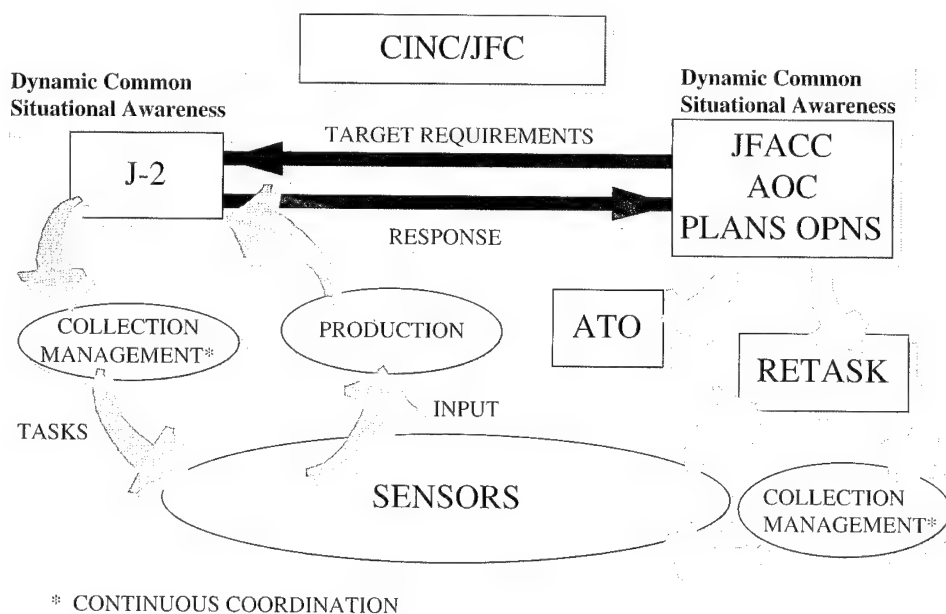


Figure 22. Requirements and response flows

Technology For Information In Warfare

This vision requires a significant leap ahead in military informational technology over that which exists today. Automated processing of individual sensor input will become faster and capable of discerning priority command information needs. Fusion will be a reality, with heretofore disparate data inputs providing operationally significant and quickly understandable, holistic situational views. Commanders will be able to select his perspective of the situation and view it from various angles, inputs of which will be provided by sensor, operational, and data base outputs. Automated target recognition will provide the ability for staring sensors to cue shooters on to commander designated high priority targets. Imbedded simulations will provide the means to project from the near-real time, accurate situational picture to alternative futures based on several potential courses of action. Simulations would provide the means to train and to mission plan and rehearse before an operation begins, but would create the virtual environment in which commanders who are in fact operating could see the results of their decisions before they make them.

Doctrinal and organizational paradigms will also be determined by how information is used and moved in the future. Because information requirements also drive communications capacity, and conversely, communications sometimes becomes the limiting factor in moving information distributed data bases might serve as one plausible solution. Ironically, the further down the tactical chain a commander is, the more specific detail he needs, and the less communications capability there is. One solution is to imbed high data base capability on each platform that would contain required operational data with change data the only input required. That would allow for robust backbone networks to serve high order commanders and provide the tactical pilot, for example, his particular common, dynamic picture. Distributed data bases, interactive through their inputs, would give even tactical commanders the informational agility to shape their particular picture of battlespace at the time and place they need it. These technological advances—automated sensor processing, dynamic fusion, automated target recognition, advanced planning and operational simulations and distributed, interactive data bases—concomitant with improved communications will provide the bases for realizing the vision for Information in Warfare, described in this document.

Command Qualities

Enduring command qualities will continue to mark superb warrior leaders. While in the years beyond 2020, computers will make more decisions for commanders, superb leaders will still be characterized by their intellectual agility, innovation, mental discipline and intuition. Knowledge-based operations will demand of commanders high technical proficiency on cyber-operations. Command will center on knowledge and insight rather than capabilities and seeing the battlefield. The technique and art of massing of operational effects will replace maneuver and fires. The art of command will be measured by gaining and maintaining informational dominance, the essential ingredient in maintaining the momentum in the information age. This 21st century commander will plan and execute independent operations using versatile information systems, risk taking actions, and intuitive response which recognize and advantage opportunity, so though computers will increasingly assist in decision-making, commanders will retain those control measures central to accomplish intent. In sum, commanders will focus the effort, synchronize effects, control information, and lead by example. Computer technology will allow

for more accuracy, timeliness, and clarity, but the commander will retain the elements and essence of decision.

Summary

This paper asserts that the defining element of warfare in the information age is the use by commanders of Information in Warfare. Information dominance in all its implications will change, fundamentally how military operations will be carried out in the 21st century. To get to that point where planning and operations move at high pace and accuracy, and where commands will dominate the information domain, there will have to be significant investments in technology areas and also in doctrinal development. Informational technology will influence doctrine in a major way; however, doctrine provides the means to apply technology smartly to military operational environments and to highlight the significant changes and seams created by the infusion of technology.

The Information in Warfare Age, (upon us now), requires well-thought through, integrated, and standard doctrine for both the Joint Force and the service component combat commanders. In an age in which command and control, by definition, will be dynamic, clear situational awareness in near real time becomes the critically necessary capability. That, in turn, will cause melding and integration of planning and execution functions, for example, in aerospace operations, and the blurring of staff responsibilities. The impact of these and other significant changes to the art and science of command would be forewarned, in part, through doctrinal development.

Finally, while technology will make more decisions for commanders, leaders will still be characterized by intellectual agility, innovation, mental discipline, and intuition. The 21st century warrior will retain the elements and essence of decision.

Appendix A:

Information Applications Panel Charter

The Information Applications Panel will develop an integrated vision of the future of information in warfare. Its technical areas will include data fusion, command and control, communications, information security, and information warfare. The notional end point for the Panel's considerations will be 2025. The emphasis will be on long term research agendas that support the technical areas listed above.

Areas of interest will include automated data fusion, distributed data communications, global collaboration systems, and threats to the operation of the Air Force infosphere. Separate monographs will be developed in each of these four areas. Two other monographs will be devoted to Air Force policy issues in the areas of information warfare and joint warfighting.

An introductory monograph will include a broad discussion of the future of information applications in an Air Force context. This monograph will also contain thoughts of the panel on the Air Force laboratory system in the area of information applications.

Appendix B

Panel Members and Affiliations

SAB Members

Dr. Charles L. Morefield, Chairman
President
Golden Triangle Technology, Inc.

Lt Gen Lincoln D. Faurer, USAF (Ret)
President
LDF, Inc.

Dr. Harold W. Sorenson
Bedford Group Vice President
The MITRE Corporation

Dr. Larry E. Druffel
Director, Software Engineering Institute
Carnegie Mellon University

Ad Hoc Advisors

MG John F. Stewart, Jr., USA, (Ret)
President
Cubic Applications, Inc.

Dr. Vincent Chan
Director, Communications Division
MIT/ Lincoln Laboratory

Dr. Ronald D. Haggarty
Vice President, Research and Technology
The MITRE Corporation

Senior Military Participant

Colonel Gerald Reynolds
Chief of Plans, Policy, and Evaluation
AF/INX, Pentagon, Washington, D.C.

Executive Officers

Lt Col John D. Davidson
Technology Planner
HQ Air Intelligence Agency, Kelly AFB, TX

Capt Dean F. Osgood
Executive Officer
USAF Scientific Advisory Board

Technical Editors

Lt Col John D. Davidson
Technology Planner
HQ Air Intelligence Agency, Kelly AFB, TX

Capt Kevin L. Taylor
Instructor of Political Science
Air Force Academy

Senior Civilian Participant

Mr. Dennis B. Richburg
Technical Director
HQ Air Intelligence Agency, Kelly AFB, TX

Appendix C:

Information Applications Panel Meeting Locations and Topics

21-23 March Washington, DC

- UAV CONOPS
- Tier II+/III
- Telecommunications Arch.
- Warbreaker
- MICOR

18-19 April San Antonio, TX

- AIA Overview
- JC2WC Overview
- AFIWC Overview
- C2 Protection
- Mod/Sim Capabilities

17-19 May Boston, MA

- Mod/Sim
- ATR
- DBS/Xlinks
- Adv. Network Tech.
- Media Laboratory
- Artificial Intelligence Lab.

14-16 Jun Princeton, NJ/ Washington, DC

- HDTV
- 3D Display Technology
- Virtual Reality
- F-22
- JAST
- Sensor Technology

27-28 Jun Colorado Springs, CO

- Coordinate with Info Tech Panel
- NTF Tour
- AFA Science Dept

Appendix D

List of Acronyms

Acronym	Definition
AI	Air Interdiction
AJ	Anti-Jam
AOC	Air Operations Center
ARPA	Advanced Research Projects Agency
ASD	Aerospace Systems Division
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
AWACS	Airborne Warning and Control System
BDA	Battle Damage Assessment
C ² W	Command and Control Warfare
C ⁴ I	Command, Control, Communications, Computer and Intelligence
CDM	Code-Division Multiplexed
CERT	Computer Emergency Response Team
CINC	Commander-in-Chief
CJCS	Chief, Joint Chiefs of Staff
CONUS	Continental United States (contiguous)
CORBA	Common Object Reference Broker Architecture
COTS	Commercial off the Shelf
CPES	Coordination, Planning and Execution System
DISA	Defense Information Systems Agency
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DSCS	Defense Satellite Communications System
EHF	Extremely High Frequency
FDM	Frequency-Division Multiplexed
Gbps	Gigabits per second
GBS	Global Broadcast Service

GHz	Gigahertz
GPS	Global Positioning Satellite System
HDTV	High-Definition Television
INMARSAT	International Maritime Satellite
IW	Information Warfare
J-2	Deputy Chief of Staff for intelligence, Joint Chiefs of Staff
JCS	Joint Chiefs of Staff
JFACC	Joint Forces Air Component Commander
JSTARS	Joint Surveillance, Tracking and Reconnaissance System
JTF	Joint Task Force
LPI	Low Probability of Interception
MAD	Mutual Assured Disruption
Mbps	Megabits per second
MII	Military Information Infrastructure
NCA	National Command Authority
NORAD	North American Air Defense
NSA	National Security Agency
OCA	Offensive Counter-Air
OODA	Observe, Orient, Decide, Act
QOS	Quality of Service
ROTC	Reserve Officer Training Corps
S&P 500	Standard and Poor's 500
SATCOM	Satellite Communication
SecDef	Secretary of Defense
SIGINT	Signals Intelligence
SONET	Synchronous Optical Network
T1	Telephone line capable of handling 1.544 megabits per second
TCP	Transfer Control Protocol
TDM	Time-division Multiplexed
UAV	Unmanned Aerospace Vehicle
WDM	Wavelength-Division Multiplexed